

15. 3. 2004

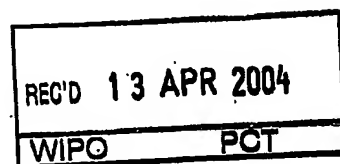
日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 月 1 7 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 0 1 0 1 8 3
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 1 0 1 8 3]



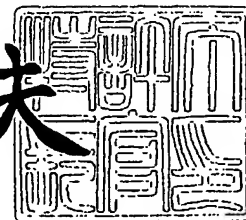
出 願 人 加 藤 誠
Applicant(s):

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2 0 0 4 年 3 月 4 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 1 6 8 2 7

【書類名】 特許願
【整理番号】 P10420T0
【あて先】 特許庁長官 太田 信一郎 殿
【国際特許分類】 H09C 1/00
H04L 9/00

【発明者】

【住所又は居所】 東京都葛飾区東金町 1 - 3 6 - 1 - 1 3 1 8

【氏名】 加藤 誠

【特許出願人】

【識別番号】 500400700

【氏名又は名称】 加藤 誠

【代理人】

【識別番号】 100088580

【弁理士】

【氏名又は名称】 秋山 敦

【選任した代理人】

【識別番号】 100111109

【弁理士】

【氏名又は名称】 城田 百合子

【手数料の表示】

【予納台帳番号】 027421

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0115949

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ送信システム及びデータ送信方法並びに装置

【特許請求の範囲】

【請求項 1】 送信側装置から受信側装置へ第 1 の換算定数、第 2 の換算定数及び第 3 の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信システムであって、

前記送信側装置は、前記第 1 の換算定数、前記第 2 の換算定数及び前記第 3 の換算定数を選択する換算定数選択手段と、前記第 2 の換算定数、又は前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 1 の代替値に暗号化し前記第 1 の換算定数、又は前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 2 の代替値へ暗号化する暗号化手段と、前記第 1 の代替値及び前記第 1 の換算定数を含む第 1 信号を生成する第 1 信号生成手段と、前記第 3 の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第 2 の代替値、前記第 2 の換算定数及び前記パターン換算定数を含む第 2 信号を生成する第 2 信号生成手段と、前記第 1 信号を前記受信側装置へ送信し前記第 2 信号を中継装置へ送信する送信手段と、を備え、

前記中継装置は、前記パターン換算定数に対応する第 3 の換算定数を記憶する記憶手段と、前記第 2 信号を受信して該第 2 信号に含まれるパターン換算定数に対応する前記第 3 の換算定数に変換して第 2' 信号を生成する信号生成手段と、前記第 2' 信号を前記受信側装置へ送信する送信手段と、を備え、

前記受信側装置は、前記送信側装置からの前記第 1 信号及び前記中継装置からの第 2' 信号を受信して前記第 1 信号から前記第 1 の代替値及び前記第 1 の換算定数、前記第 2' 信号から前記第 2 の代替値、前記第 2 の換算定数及び前記第 3 の換算定数を読取る読取手段と、前記第 1 の代替値及び前記第 2 の代替値をそれぞれ暗号化に用いられた換算定数によって第 1 の復号化データ及び第 2 の復号化データへ復号化する復号化手段と、前記第 1 の復号化データと前記第 2 の復号化データから前記第 1 信号及び前記第 2' 信号を受け入れる認証をする認証手段と、を備えたことを特徴とするデータ送信システム。

【請求項 2】 送信側装置から受信側装置へ第 1 の換算定数、第 2 の換算定

数、第3の換算定数及び第4の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信システムであって、

前記送信側装置は、前記第1の換算定数、前記第2の換算定数、前記第3の換算定数及び前記第4の換算定数を選択する換算定数選択手段と、前記第2の換算定数及び前記第4の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化手段と、前記第3の換算定数及び第4の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は前記第4の換算定数に対応するパターン換算定数を含む第1信号を生成する第1信号生成手段と、前記第2の代替値、前記第2の換算定数、及び前記第1信号に含まれない前記第3の換算定数又は前記第4の換算定数のパターン換算定数を含む第2信号を生成する第2信号生成手段と、前記第1信号を第1の中継装置へ送信し前記第2信号を第2の中継装置へ送信する送信手段と、を備え、

前記第1の中継装置は、前記パターン換算定数に対応する第3の換算定数又は第4の換算定数を記憶する記憶手段と、前記第1信号を受信して該信号に含まれるパターン換算定数に対応する前記第3の換算定数又は第4の換算定数に変換して第1'信号を生成する信号生成手段と、前記第1'信号を前記受信側装置へ送信する送信手段と、を備え、

前記第2の中継装置は、前記パターン換算定数に対応する第3の換算定数又は第4の換算定数を記憶する記憶手段と、前記第2信号を受信して該信号に含まれるパターン換算定数に対応する前記第3の換算定数又は第4の換算定数に変換して第2'信号を生成する信号生成手段と、前記第2'信号を前記受信側装置へ送信する送信手段と、を備え、

前記受信側装置は、前記第1'信号及び前記第2'信号を受信して前記第1'信号から前記第1の代替値、前記第1の換算定数及び前記第3の換算定数又は第4の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数及び前記第3の換算定数又は第4の換算定数を読取る読取手段と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復

号化データ及び第2の復号化データへ復号化する復号化手段と、前記第1の複合化データと前記第2の復号化データから前記第1'信号及び前記第2'信号を受け入れる認証をする認証手段と、を備えたことを特徴とするデータ送信システム。

【請求項3】 送信側装置から受信側装置へ第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信システムであって、

前記送信側装置は、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択する換算定数選択手段と、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化手段と、前記第1の代替値及び前記第1の換算定数を含む第1信号を生成する第1信号生成手段と、前記第3の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を含む第2信号を生成する第2信号生成手段と、前記第1信号及び前記第2信号を前記受信側装置へ送信する送信手段と、を備え、

前記受信側装置は、前記第1信号及び前記第2信号を受信して前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2信号から前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を読取る読取手段と、前記パターン換算定数に対応する第3の換算定数を記憶する記憶手段と、前記読取られたパターン換算定数から前記第3の換算定数を読取る手段と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化手段と、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2信号を受け入れる認証をする認証手段と、を備えたことを特徴とするデータ送信システム。

【請求項4】 前記暗号化手段は、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化することを特徴と

する請求項 1 又は 3 に記載のデータ送信システム。

【請求項 5】 前記暗号化手段は、前記第 2 の換算定数を用いて前記送信データを前記第 1 の代替値へ暗号化し、前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記第 2 の代替値へ暗号化することを特徴とする請求項 1 又は 3 に記載のデータ送信システム。

【請求項 6】 前記暗号化手段は、前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを前記第 1 の代替値へ暗号化し、前記第 1 の換算定数を用いて前記第 2 の代替値へ暗号化することを特徴とする請求項 1 又は 3 に記載のデータ送信システム。

【請求項 7】 前記受信側装置は、前記第 1 の復号化データ又は第 2 の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出手段を備えたことを特徴とする請求項 1 乃至 3 のいずれかに記載のデータ送信システム。

【請求項 8】 前記認証手段は、前記第 1 の複合化データと前記第 2 の復号化データが一致したときに前記認証を行うことを特徴とする請求項 1 乃至 3 のいずれかに記載のデータ送信システム。

【請求項 9】 前記送信側装置、前記中継装置及び前記受信側装置は、インターネットを含む通信回線網に接続されたことを特徴とする請求項 1 又は 2 に記載のデータ送信システム。

【請求項 10】 前記送信側装置と受信側装置は、赤外線方式、無線電波方式、光通信方式、有線通信方式のいずれかによって前記信号の送受信を行うことを特徴とする請求項 3 に記載のデータ送信システム。

【請求項 11】 送信側装置から受信側装置へ第 1 の換算定数、第 2 の換算定数及び第 3 の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信方法であって、

前記送信側装置が、前記第 1 の換算定数、前記第 2 の換算定数及び前記第 3 の換算定数を選択するステップと、

前記送信側装置が、前記第 2 の換算定数、又は前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 1 の代替値に暗号化し前記第 1 の換算

定数、又は前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 2 の代替値へ暗号化する暗号化ステップと、

前記送信側装置が、前記第 1 の代替値、及び前記第 1 の換算定数を含む第 1 信号を生成する第 1 信号生成ステップと、

前記送信側装置が、前記第 2 の代替値、前記第 2 の換算定数、及び前記第 3 の換算定数に対応するパターン換算定数を含む第 2 信号を生成する第 2 信号生成ステップと、

前記送信側装置が、前記第 1 信号を前記受信側装置へ送信し前記第 2 信号を中継装置へ送信する第 1 送信ステップと、

前記中継装置が、前記第 2 信号を受信して該第 2 信号に含まれるパターン換算定数に対応する前記第 3 の換算定数に変換して第 2' 信号を生成する変換ステップと、

前記中継装置が、前記第 2' 信号を前記受信側装置へ送信する第 2 送信ステップと、

前記受信側装置が、前記送信側装置からの前記第 1 信号及び前記中継装置からの第 2' 信号を受信して前記第 1 信号から前記第 1 の代替値、及び前記第 1 の換算定数、前記第 2' 信号から前記第 2 の代替値、前記第 2 の換算定数、及び前記第 3 の換算定数を読取る読取ステップと、

前記受信側装置が、前記第 1 の代替値及び前記第 2 の代替値をそれぞれ暗号化に用いられた換算定数によって第 1 の復号化データ及び第 2 の復号化データへ復号化する復号化ステップと、

前記受信側装置が、前記第 1 の複合化データと前記第 2 の復号化データから前記第 1 信号及び前記第 2' 信号を受け入れる認証をする認証ステップと、を備えたことを特徴とするデータ送信方法。

【請求項 12】 送信側装置から受信側装置へ第 1 の換算定数、第 2 の換算定数、第 3 の換算定数及び第 4 の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信方法であって、

前記送信側装置が、前記第 1 の換算定数、前記第 2 の換算定数、前記第 3 の換算定数及び前記第 4 の換算定数を選択するステップと、

前記送信側装置が、前記第 2 の換算定数、及び前記第 4 の換算定数を用いて前記送信データを第 1 の代替値に暗号化し前記第 1 の換算定数、及び前記第 3 の換算定数を用いて前記送信データを第 2 の代替値へ暗号化する暗号化ステップと、

前記送信側装置が、前記第 1 の代替値、前記第 1 の換算定数、及び前記第 3 の換算定数又は前記第 4 の換算定数に対応するパターン換算定数を含む第 1 信号を生成する第 1 信号生成ステップと、

前記送信側装置が、前記第 2 の代替値、前記第 2 の換算定数、及び前記第 1 信号に含まれない前記第 3 の換算定数又は前記第 4 の換算定数のパターン換算定数を含む第 2 信号を生成する第 2 信号生成ステップと、

前記送信側装置が、前記第 1 信号を第 1 の中継装置へ送信し前記第 2 信号を第 2 の中継装置へ送信する第 1 送信ステップと、

前記第 1 の中継装置及び前記第 2 の中継装置が、前記第 1 信号又は前記第 2 信号を受信して該信号に含まれるパターン換算定数に対応する前記第 3 の換算定数又は第 4 の換算定数に変換して第 1' 信号又は第 2' 信号を生成する変換ステップと、

前記第 1 の中継装置及び前記第 2 の中継装置が、前記第 1' 信号又は前記第 2' 信号を前記受信側装置へ送信する第 2 送信ステップと、

前記受信側装置が、前記第 1' 信号及び前記第 2' 信号を受信して前記第 1' 信号から前記第 1 の代替値、前記第 1 の換算定数、及び前記第 3 の換算定数又は第 4 の換算定数、前記第 2' 信号から前記第 2 の代替値、前記第 2 の換算定数、及び前記第 3 の換算定数又は第 4 の換算定数を読取る読取ステップと、

前記受信側装置が、前記第 1 の代替値及び前記第 2 の代替値をそれぞれ暗号化に用いられた換算定数によって第 1 の復号化データ及び第 2 の復号化データへ復号化する復号化ステップと、

前記受信側装置が、前記第 1 の複合化データと前記第 2 の復号化データから前記第 1' 信号及び前記第 2' 信号を受け入れる認証をする認証ステップと、を備えたことを特徴とするデータ送信方法。

【請求項 13】 送信側装置から受信側装置へ第 1 の換算定数、第 2 の換算定数及び第 3 の換算定数の少なくとも一の換算定数によって暗号化された送信デ

ータを送信するデータ送信方法であって、

前記送信側装置が、前記第 1 の換算定数、前記第 2 の換算定数及び前記第 3 の換算定数を選択するステップと、

前記送信側装置が、前記第 2 の換算定数、又は前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 1 の代替値に暗号化し前記第 1 の換算定数、又は前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 2 の代替値へ暗号化する暗号化ステップと、

前記送信側装置が、前記第 1 の代替値及び前記第 1 の換算定数を含む第 1 信号を生成する第 1 信号生成ステップと、

前記送信側装置が、前記第 2 の代替値、前記第 2 の換算定数及び前記第 3 の換算定数に対応するパターン換算定数を含む第 2 信号を生成する第 2 信号生成ステップと、

前記送信側装置が、前記第 1 信号及び前記第 2 信号を前記受信側装置へ送信する送信ステップと、

前記受信側装置が、前記第 1 信号及び前記第 2 信号を受信して前記第 1 信号から前記第 1 の代替値及び前記第 1 の換算定数、前記第 2 信号から前記第 2 の代替値、前記第 2 の換算定数及び前記パターン換算定数を読取る読取ステップと、

前記受信側装置が、前記読取られたパターン換算定数に対応する前記第 3 の換算定数を取得する換算定数取得ステップと、

前記受信側装置が、前記第 1 の代替値及び前記第 2 の代替値をそれぞれ暗号化に用いられた換算定数によって第 1 の復号化データ及び第 2 の復号化データへ復号化する復号化ステップと、

前記受信側装置が、前記第 1 の複合化データと前記第 2 の復号化データから前記第 1 信号及び前記第 2 信号を受け入れる認証をする認証ステップと、を備えたことを特徴とするデータ送信方法。

【請求項 14】 前記暗号化ステップでは、前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを前記第 1 の代替値へ暗号化し、前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記第 2 の代替値へ暗号化することを特徴とする請求項 11 又は 13 に記載のデータ送信方法。

【請求項 15】 前記暗号化ステップでは、前記第 2 の換算定数を用いて前記送信データを前記第 1 の代替値へ暗号化し、前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記第 2 の代替値へ暗号化することを特徴とする請求項 11 又は 13 に記載のデータ送信方法。

【請求項 16】 前記暗号化ステップでは、前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを前記第 1 の代替値へ暗号化し、前記第 1 の換算定数を用いて前記第 2 の代替値へ暗号化することを特徴とする請求項 11 又は 13 に記載のデータ送信方法。

【請求項 17】 前記認証ステップの後、前記第 1 の復号化データ又は第 2 の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出ステップを備えたことを特徴とする請求項 11 乃至 13 のいずれかに記載のデータ送信方法。

【請求項 18】 前記認証ステップでは、前記第 1 の複合化データと前記第 2 の復号化データが一致したときに前記認証を行うことを特徴とする請求項 11 乃至 13 のいずれかに記載のデータ送信方法。

【請求項 19】 第 1 の換算定数、第 2 の換算定数及び第 3 の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信する装置であって、

前記換算定数に対応するパターン換算定数を記憶する記憶部と、

前記第 1 の換算定数、前記第 2 の換算定数及び前記第 3 の換算定数を選択する換算定数選択処理と、前記第 2 の換算定数、又は前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 1 の代替値に暗号化し前記第 1 の換算定数、又は前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 2 の代替値へ暗号化する暗号化処理と、前記第 1 の代替値、及び前記第 1 の換算定数を含む第 1 信号を生成する第 1 信号生成処理と、前記第 2 の代替値、前記第 2 の換算定数、及び前記第 3 の換算定数に対応するパターン換算定数を含む第 2 信号を生成する第 2 信号生成処理と、前記第 1 信号と前記第 2 信号をそれぞれ送信する処理と、を行う制御部と、

前記第 1 信号と前記第 2 信号を外部へ送信する送信部と、を備えたことを特徴

とする装置。

【請求項 20】 前記制御部は、前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを前記第 1 の代替値へ暗号化し、前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記第 2 の代替値へ暗号化することを特徴とする請求項 19 に記載の装置。

【請求項 21】 前記制御部は、前記第 2 の換算定数を用いて前記送信データを前記第 1 の代替値へ暗号化し、前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記第 2 の代替値へ暗号化することを特徴とする請求項 19 に記載の装置。

【請求項 22】 前記制御部は、前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを前記第 1 の代替値へ暗号化し、前記第 1 の換算定数を用いて前記第 2 の代替値へ暗号化することを特徴とする請求項 19 に記載の装置。

【請求項 23】 第 1 の換算定数、第 2 の換算定数、第 3 の換算定数及び第 4 の換算定数のうち二の換算定数によって暗号化された送信データを送信する装置であって、

前記換算定数に対応するパターン換算定数を記憶する記憶部と、

前記第 1 の換算定数、前記第 2 の換算定数、前記第 3 の換算定数及び前記第 4 の換算定数を選択する換算定数選択処理と、前記第 2 の換算定数及び前記第 4 の換算定数を用いて前記送信データを第 1 の代替値に暗号化し前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 2 の代替値へ暗号化する暗号化処理と、前記第 1 の代替値、前記第 1 の換算定数、及び前記第 3 の換算定数又は前記第 4 の換算定数に対応するパターン換算定数を含む第 1 信号を生成する第 1 信号生成処理と、前記第 2 の代替値、前記第 2 の換算定数、及び前記第 1 信号に含まれない前記第 3 の換算定数又は前記第 4 の換算定数のパターン換算定数を含む第 2 信号を生成する第 2 信号生成処理と、を行う制御部と、

前記第 1 信号と前記第 2 信号を外部へ送信する送信部と、を備えたことを特徴とする装置。

【請求項 24】 送信データの暗号化に用いられる換算定数に対応するパタ

ー換算定数を含む信号を転送する装置であって、
前記換算定数に対応するパターン換算定数を記憶する記憶部と、
前記信号を送受信する送受信部と、
受信した前記信号に含まれるパターン換算定数に対応する前記換算定数に変換して前記信号を変換する信号生成処理と、前記変換された信号を転送する処理と、
を行う制御部と、を備えたことを特徴とする装置。

【請求項 25】 第 1 の換算定数、第 2 の換算定数及び第 3 の換算定数の少なくとも一の換算定数によって暗号化された送信データを含む第 1 信号と第 2 信号を受信して送信データを復号化する装置であって、

前記第 1 信号には、前記第 2 の換算定数、又は前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データが暗号化された第 1 の代替値と、第 1 の換算定数と、が含まれ、

前記第 2 信号には、前記第 1 の換算定数、又は前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記送信データが暗号化された第 2 の代替値と、前記第 2 の換算定数と、前記第 3 の換算定数と、が含まれ、

前記第 1 信号及び前記第 2 信号を受信する受信部と、

受信した前記第 1 信号から前記第 1 の代替値及び前記第 1 の換算定数、前記第 2 信号から前記第 2 の代替値、前記第 2 の換算定数及び前記第 3 の換算定数を読取る処理と、前記第 1 の代替値及び前記第 2 の代替値をそれぞれ暗号化に用いられた換算定数によって第 1 の復号化データ及び第 2 の復号化データへ復号化する復号化処理と、前記第 1 の複合化データと前記第 2 の復号化データから前記第 1 信号及び前記第 2 信号を受け入れる認証をする認証処理と、を行う制御部と、を備えたことを特徴とする装置。

【請求項 26】 第 1 の換算定数、第 2 の換算定数、第 3 の換算定数及び第 4 の換算定数のうち二の換算定数によって暗号化された送信データを含む第 1 信号と第 2 信号を受信して送信データを復号する装置であって、

前記第 1 信号には、前記第 2 の換算定数及び前記第 4 の換算定数を用いて前記送信データが暗号化された第 1 の代替値と、前記第 1 の換算定数と、前記第 3 の換算定数又は前記第 4 の換算定数と、が含まれ、

前記第 2' 信号には、第 1 の換算定数及び前記第 3 の換算定数を用いて前記送信データが暗号化された第 1 の代替値と、第 2 の換算定数と、前記第 1' 信号に含まれていない第 3 の換算定数又は前記第 4 の換算定数と、が含まれ、

前記第 1' 信号及び前記第 2' 信号を受信する受信部と、

受信した前記第 1' 信号から前記第 1 の代替値、前記第 1 の換算定数、及び前記第 3 の換算定数又は第 4 の換算定数、前記第 2' 信号から前記第 2 の代替値、前記第 2 の換算定数、及び前記第 3 の換算定数又は第 4 の換算定数を読取る処理と、前記第 1 の代替値及び前記第 2 の代替値をそれぞれ暗号化に用いられた換算定数によって第 1 の復号化データ及び第 2 の復号化データへ復号化する復号化処理と、前記第 1 の複合化データと前記第 2 の復号化データから前記第 1' 信号及び前記第 2' 信号を受け入れる認証をする認証処理と、を行う制御部を備えたことを特徴とする装置。

【請求項 27】 第 1 の換算定数、第 2 の換算定数及び第 3 の換算定数の少なくとも一の換算定数によって暗号化された送信データを含む第 1 信号と第 2 信号を受信して送信データを復号化する装置であって、

前記第 1 信号には、前記第 2 の換算定数、又は前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データが暗号化された第 1 の代替値と、第 1 の換算定数と、が含まれ、

前記第 2 信号には、前記第 1 の換算定数、又は前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記送信データが暗号化された第 2 の代替値と、前記第 2 の換算定数と、前記第 3 の換算定数に対応するパターン換算定数と、が含まれ、

前記換算定数に対応するパターン換算定数を記憶する記憶部と、

前記第 1 信号及び前記第 2 信号を受信する受信部と、

前記第 1 信号から前記第 1 の代替値、及び前記第 1 の換算定数、前記第 2 信号から前記第 2 の代替値、前記第 2 の換算定数、及び前記パターン換算定数を読取る処理と、前記読取られたパターン換算定数から前記第 3 の換算定数を取得する処理と、前記第 1 の代替値及び前記第 2 の代替値をそれぞれ暗号化に用いられた換算定数によって第 1 の復号化データ及び第 2 の復号化データへ復号化する復号化処理と、前記第 1 の複合化データと前記第 2 の復号化データから前記第 1 信号

及び前記第2信号を受け入れる認証をする認証処理と、を行う制御部と、を備えたことを特徴とする装置。

【請求項28】 前記制御部は、前記第1の復号化データ又は第2の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出することを特徴とする請求項25乃至27のいずれかに記載の装置。

【請求項29】 前記制御部は、前記第1の複合化データと前記第2の復号化データが一致したときに前記認証を行うことを特徴とする請求項25乃至27のいずれかに記載の装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、データ送信する際に送信データが漏洩した場合においても、その復号化が困難であると共に、第3者の成りすまし送信による不都合を回避できるデータ送信システム及びデータ送信方法並びに装置に関する。

【0002】

【従来の技術】

従来から、送信者側で送信すべきデータの暗号化を行い、該暗号化データと該暗号化データを復号化するための暗号鍵とを別々の回線（例えば、衛星通信回線と地上回線）によって受信者側へ送信する技術がある。（例えば、特許文献1参照）。

【0003】

受信者側では、暗号化されたデータと暗号鍵とを別々に受信し、これらにより元のデータを復号化することができる。このように別々の回線で暗号化データと暗号鍵が送信されることにより、データ送信の秘匿性を高めることができる。

【0004】

【特許文献1】

特許第3052322号公報（第2-3頁、第1-2図）

【0005】

【発明が解決しようとする課題】

しかし、受信者は、暗号鍵と暗号化されたデータの送信者を認証することなくデータを受信するため、本来送信するはずの送信者に成り代わって第3者によって送信されても送信データを認証することができなかった。

【0006】

インターネット等の通信回線上においては、個人認証を行う認証サービス会社の個人認証サービスもある。しかし、そのような認証サービス会社による個人認証サービスは高価であり、個人が利用するには不向きであった。

【0007】

本発明は、上記課題を解決するためになされたものであり、本来の送信者になりかわって第3者がデータを送信しても、受信者側で送信データの認証を行うことができ、上記成りすまし送信による不都合を防ぐことができるデータ送信システム及びデータ送信方法並びに装置を提供することにある。

【0008】

【課題を解決するための手段】

上記課題は請求項1に記載のデータ送信システムによれば、送信側装置から受信側装置へ第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信システムであって、前記送信側装置は、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択する換算定数選択手段と、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化手段と、前記第1の代替値及び前記第1の換算定数を含む第1信号を生成する第1信号生成手段と、前記第3の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を含む第2信号を生成する第2信号生成手段と、前記第1信号を前記受信側装置へ送信し前記第2信号を中継装置へ送信する送信手段と、を備え、前記中継装置は、前記パターン換算定数に対応する第3の換算定数を記憶する記憶手段と、前記第2信号を受信して該第2信号に含まれるパターン換算定数に対応する前記第3の換算定数に変換

して第2'信号を生成する信号生成手段と、前記第2'信号を前記受信側装置へ送信する送信手段と、を備え、前記受信側装置は、前記送信側装置からの前記第1信号及び前記中継装置からの第2'信号を受信して前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数及び前記第3の換算定数を読取る読取手段と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化手段と、前記第1の復号化データと前記第2の復号化データから前記第1信号及び前記第2'信号を受け入れる認証をする認証手段と、を備えることにより解決される。

【0009】

このように本発明によれば、第1信号に含まれる暗号化データを暗号化した第2の換算定数は第2信号に含めて送信され、第2信号に含まれる暗号化データを暗号化した第1の換算定数は第1信号に含めて送信される。

【0010】

さらに、第3の換算定数そのものは送信されず、第3の換算定数に対応するパターン換算定数が第2信号に含めて中継装置へ送信される。そして、このパターン換算定数が、中継装置で第3の換算定数へ変換されることにより、第2信号が第2'信号に変換され、受信側へ転送される。

【0011】

このように送信することにより、第3者は第1信号及び第2信号の双方を取得したとしてもパターン換算定数が不明であるので、送信データの復号化を行うことはできない。また、第3者が第1信号又は第2'信号の一方を取得したとしても、それぞれの信号には換算定数のすべての換算定数が含まれていないので、復号化を行うことはできない。

【0012】

さらに、第3者が第1信号及び第2'信号の双方を取得したとしても、復号化方法を取得しない限り、有意な復号化データを得ることはできない。

【0013】

以上のように、本発明によれば第3者が暗号化データを不正に取得したとして

も、暗号化データの復号化を有意に行うことができず、送信データの秘匿性を高めることができる。

【0014】

また、受信側装置では、送信側装置で選択されたパターン換算定数を知らなくても暗号化データを復号化することができる。したがって、送信側装置では複数のパターン換算定数及び換算定数の組合せを設定することにより、複数の受信側装置へ暗号化データを送信する場合にも秘匿性を高めることができる。

【0015】

そして、第3者には換算定数による暗号化方法及びパターン換算定数が不明であるため、送信者に成り代わって送信したとしても、受信側装置では有意なデータとして復号化することができないか、復号化データが一致しないので、成りすまし送信による不都合を回避することができる。

【0016】

また、上記課題は、請求項2のデータ送信システムによれば、送信側装置から受信側装置へ第1の換算定数、第2の換算定数、第3の換算定数及び第4の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信システムであって、前記送信側装置は、前記第1の換算定数、前記第2の換算定数、前記第3の換算定数及び前記第4の換算定数を選択する換算定数選択手段と、前記第2の換算定数及び前記第4の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化手段と、前記第3の換算定数及び第4の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は前記第4の換算定数に対応するパターン換算定数を含む第1信号を生成する第1信号生成手段と、前記第2の代替値、前記第2の換算定数、及び前記第1信号に含まれない前記第3の換算定数又は前記第4の換算定数のパターン換算定数を含む第2信号を生成する第2信号生成手段と、前記第1信号を第1の中継装置へ送信し前記第2信号を第2の中継装置へ送信する送信手段と、を備え、前記第1の中継装置は、前記パターン換算定数に対応する第3の換算定数又は第4の換算定数を記憶する記憶手段と

、前記第 1 信号を受信して該信号に含まれるパターン換算定数に対応する前記第 3 の換算定数又は第 4 の換算定数に変換して第 1' 信号を生成する信号生成手段と、前記第 1' 信号を前記受信側装置へ送信する送信手段と、を備え、前記第 2 の中継装置は、前記パターン換算定数に対応する第 3 の換算定数又は第 4 の換算定数を記憶する記憶手段と、前記第 2 信号を受信して該信号に含まれるパターン換算定数に対応する前記第 3 の換算定数又は第 4 の換算定数に変換して第 2' 信号を生成する信号生成手段と、前記第 2' 信号を前記受信側装置へ送信する送信手段と、を備え、前記受信側装置は、前記第 1' 信号及び前記第 2' 信号を受信して前記第 1' 信号から前記第 1 の代替値、前記第 1 の換算定数及び前記第 3 の換算定数又は第 4 の換算定数、前記第 2' 信号から前記第 2 の代替値、前記第 2 の換算定数及び前記第 3 の換算定数又は第 4 の換算定数を読取る読取手段と、前記第 1 の代替値及び前記第 2 の代替値をそれぞれ暗号化に用いられた換算定数によって第 1 の復号化データ及び第 2 の復号化データへ復号化する復号化手段と、前記第 1 の複合化データと前記第 2 の復号化データから前記第 1' 信号及び前記第 2' 信号を受け入れる認証をする認証手段と、を備えることにより解決される。

【0017】

このように本発明によれば、請求項 1 に記載の発明に加え、第 1 信号も中継装置を介して受信側装置へ転送される。これにより、さらにデータ送信の秘匿性が高まり、又、より効果的に成りすまし送信による不都合を排除することができる。

【0018】

また、上記課題は、請求項 3 に記載のデータ送信システムによれば、送信側装置から受信側装置へ第 1 の換算定数、第 2 の換算定数及び第 3 の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信システムであって、前記送信側装置は、前記第 1 の換算定数、前記第 2 の換算定数及び前記第 3 の換算定数を選択する換算定数選択手段と、前記第 2 の換算定数、又は前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 1 の代替値に暗号化し前記第 1 の換算定数、又は前記第 1 の換算定数及び前記第 3 の

換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化手段と、前記第1の代替値及び前記第1の換算定数を含む第1信号を生成する第1信号生成手段と、前記第3の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を含む第2信号を生成する第2信号生成手段と、前記第1信号及び前記第2信号を前記受信側装置へ送信する送信手段と、を備え、前記受信側装置は、前記第1信号及び前記第2信号を受信して前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2信号から前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を読取る読取手段と、前記パターン換算定数に対応する第3の換算定数を記憶する記憶手段と、前記読取られたパターン換算定数から前記第3の換算定数を読取る手段と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化手段と、前記第1の復号化データと前記第2の復号化データから前記第1信号及び前記第2信号を受け入れる認証をする認証手段と、を備えることにより解決される。

【0019】

このように本発明によれば、請求項1に記載の発明と異なり、中継装置を設けることなく、中継装置が行っていたパターン換算定数を換算定数に変換する処理を受信側装置で行うように構成されている。このようにすることにより、データの秘匿性を低下させることなく、また、成りすまし送信による不都合を排除することができると共に、システムの構成を簡単化することができる。

【0020】

また、請求項4に記載のように、前記暗号化手段は、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化するように構成することができる。

【0021】

また、請求項5に記載のように、前記暗号化手段は、前記第2の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前

記第3の換算定数を用いて前記第2の代替値へ暗号化するように構成することができる。

【0022】

また、請求項6に記載のように、前記暗号化手段は、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数を用いて前記第2の代替値へ暗号化すれば、成りすまし送信による2つの信号が受信側装置へ送信されてきた場合であっても、それぞれの信号を復号して得られた復号化データは不一致となるので、成りすまし送信を排除する効果が高まるので好適である。

【0023】

また、請求項7に記載のように、前記受信側装置は、前記第1の復号化データ又は第2の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出手段を備えれば、本システムのデータ秘匿性及び成りすまし送信排除効果より、本人又は受信信号を認証して外部駆動装置を操作することができるので好適である。

【0024】

また、請求項8に記載のように、前記認証手段は、前記第1の複合化データと前記第2の復号化データが一致したときに前記認証を行うように構成することができる。また、請求項9に記載のように、前記送信側装置、前記中継装置及び前記受信側装置は、インターネットを含む通信回線網に接続する構成とすることができる。また、請求項10に記載のように、前記送信側装置と受信側装置は、赤外線方式、無線電波方式、光通信方式、有線通信方式のいずれかによって前記信号の送受信を行うことが可能である。

【0025】

また、請求項11に記載のように、本発明のデータ送信方法は、送信側装置から受信側装置へ第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信方法であって、前記送信側装置が、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択するステップと、前記送信側装置が、前記第2の換算定数、

又は前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 1 の代替値に暗号化し前記第 1 の換算定数、又は前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 2 の代替値へ暗号化する暗号化ステップと、前記送信側装置が、前記第 1 の代替値、及び前記第 1 の換算定数を含む第 1 信号を生成する第 1 信号生成ステップと、前記送信側装置が、前記第 2 の代替値、前記第 2 の換算定数、及び前記第 3 の換算定数に対応するパターン換算定数を含む第 2 信号を生成する第 2 信号生成ステップと、前記送信側装置が、前記第 1 信号を前記受信側装置へ送信し前記第 2 信号を中継装置へ送信する第 1 送信ステップと、前記中継装置が、前記第 2 信号を受信して該第 2 信号に含まれるパターン換算定数に対応する前記第 3 の換算定数に変換して第 2' 信号を生成する変換ステップと、前記中継装置が、前記第 2' 信号を前記受信側装置へ送信する第 2 送信ステップと、前記受信側装置が、前記送信側装置からの前記第 1 信号及び前記中継装置からの第 2' 信号を受信して前記第 1 信号から前記第 1 の代替値、及び前記第 1 の換算定数、前記第 2' 信号から前記第 2 の代替値、前記第 2 の換算定数、及び前記第 3 の換算定数を読取る読取ステップと、前記受信側装置が、前記第 1 の代替値及び前記第 2 の代替値をそれぞれ暗号化に用いられた換算定数によって第 1 の復号化データ及び第 2 の復号化データへ復号化する復号化ステップと、前記受信側装置が、前記第 1 の複合化データと前記第 2 の復号化データから前記第 1 信号及び前記第 2' 信号を受け入れる認証をする認証ステップと、を備えるものとすることができる。

【0026】

また、請求項 12 に記載のように、本発明のデータ送信方法は、送信側装置から受信側装置へ第 1 の換算定数、第 2 の換算定数、第 3 の換算定数及び第 4 の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信方法であって、前記送信側装置が、前記第 1 の換算定数、前記第 2 の換算定数、前記第 3 の換算定数及び前記第 4 の換算定数を選択するステップと、前記送信側装置が、前記第 2 の換算定数、及び前記第 4 の換算定数を用いて前記送信データを第 1 の代替値に暗号化し前記第 1 の換算定数、及び前記第 3 の換算定数を用いて前記送信データを第 2 の代替値へ暗号化する暗号化ステップと、前記送信側

装置が、前記第 1 の代替値、前記第 1 の換算定数、及び前記第 3 の換算定数又は前記第 4 の換算定数に対応するパターン換算定数を含む第 1 信号を生成する第 1 信号生成ステップと、前記送信側装置が、前記第 2 の代替値、前記第 2 の換算定数、及び前記第 1 信号に含まれない前記第 3 の換算定数又は前記第 4 の換算定数のパターン換算定数を含む第 2 信号を生成する第 2 信号生成ステップと、前記送信側装置が、前記第 1 信号を第 1 の中継装置へ送信し前記第 2 信号を第 2 の中継装置へ送信する第 1 送信ステップと、前記第 1 の中継装置及び前記第 2 の中継装置が、前記第 1 信号又は前記第 2 信号を受信して該信号に含まれるパターン換算定数に対応する前記第 3 の換算定数又は第 4 の換算定数に変換して第 1' 信号又は第 2' 信号を生成する変換ステップと、前記第 1 の中継装置及び前記第 2 の中継装置が、前記第 1' 信号又は前記第 2' 信号を前記受信側装置へ送信する第 2 送信ステップと、前記受信側装置が、前記第 1' 信号及び前記第 2' 信号を受信して前記第 1' 信号から前記第 1 の代替値、前記第 1 の換算定数、及び前記第 3 の換算定数又は第 4 の換算定数、前記第 2' 信号から前記第 2 の代替値、前記第 2 の換算定数、及び前記第 3 の換算定数又は第 4 の換算定数を読取る読取ステップと、前記受信側装置が、前記第 1 の代替値及び前記第 2 の代替値をそれぞれ暗号化に用いられた換算定数によって第 1 の復号化データ及び第 2 の復号化データへ復号化する復号化ステップと、前記受信側装置が、前記第 1 の復号化データと前記第 2 の復号化データから前記第 1' 信号及び前記第 2' 信号を受け入れる認証をする認証ステップと、を備えるものとすることができる。

【0027】

また、請求項 13 に記載のように、本発明のデータ送信方法は、送信側装置から受信側装置へ第 1 の換算定数、第 2 の換算定数及び第 3 の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信方法であって、前記送信側装置が、前記第 1 の換算定数、前記第 2 の換算定数及び前記第 3 の換算定数を選択するステップと、前記送信側装置が、前記第 2 の換算定数、又は前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 1 の代替値に暗号化し前記第 1 の換算定数、又は前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 2 の代替値へ暗号化する暗号化ステップ

と、前記送信側装置が、前記第1の代替値及び前記第1の換算定数を含む第1信号を生成する第1信号生成ステップと、前記送信側装置が、前記第2の代替値、前記第2の換算定数及び前記第3の換算定数に対応するパターン換算定数を含む第2信号を生成する第2信号生成ステップと、前記送信側装置が、前記第1信号及び前記第2信号を前記受信側装置へ送信する送信ステップと、前記受信側装置が、前記第1信号及び前記第2信号を受信して前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2信号から前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を読取る読取ステップと、前記受信側装置が、前記読取られたパターン換算定数に対応する前記第3の換算定数を取得する換算定数取得ステップと、前記受信側装置が、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化ステップと、前記受信側装置が、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2信号を受け入れる認証をする認証ステップと、を備えるものとすることができる。

【0028】

また、請求項14に記載のように、前記暗号化ステップでは、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化するようにできる。

【0029】

また、請求項15に記載のように、前記暗号化ステップでは、前記第2の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化するようにできる。

【0030】

また、請求項16に記載のように、前記暗号化ステップでは、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数を用いて前記第2の代替値へ暗号化するようにできる。

【0031】

また、請求項17に記載のように、前記認証ステップの後、前記第1の復号化データ又は第2の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出ステップを備えれば好適である。

【0032】

また、請求項18に記載のように、前記認証ステップでは、前記第1の複合化データと前記第2の復号化データが一致したときに前記認証を行うようにできる。

【0033】

また、請求項19に記載のように、本発明は、第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信する装置であって、前記換算定数に対応するパターン換算定数を記憶する記憶部と、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択する換算定数選択処理と、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化処理と、前記第1の代替値、及び前記第1の換算定数を含む第1信号を生成する第1信号生成処理と、前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数に対応するパターン換算定数を含む第2信号を生成する第2信号生成処理と、前記第1信号と前記第2信号をそれぞれ送信する処理と、を行う制御部と、前記第1信号と前記第2信号を外部へ送信する送信部と、を備える装置により実現できる。

【0034】

また、請求項20に記載のように、前記制御部は、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化する構成とすることができる。

【0035】

また、請求項21に記載のように、前記制御部は、前記第2の換算定数を用い

て前記送信データを前記第 1 の代替値へ暗号化し、前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記第 2 の代替値へ暗号化する構成とすることができる。

【0036】

また、請求項 22 に記載のように、前記制御部は、前記第 2 の換算定数及び前記第 3 の換算定数を用いて前記送信データを前記第 1 の代替値へ暗号化し、前記第 1 の換算定数を用いて前記第 2 の代替値へ暗号化する構成とすることができる。

【0037】

また、請求項 23 に記載のように、本発明は、第 1 の換算定数、第 2 の換算定数、第 3 の換算定数及び第 4 の換算定数のうち二の換算定数によって暗号化された送信データを送信する装置であって、前記換算定数に対応するパターン換算定数を記憶する記憶部と、前記第 1 の換算定数、前記第 2 の換算定数、前記第 3 の換算定数及び前記第 4 の換算定数を選択する換算定数選択処理と、前記第 2 の換算定数及び前記第 4 の換算定数を用いて前記送信データを第 1 の代替値に暗号化し前記第 1 の換算定数及び前記第 3 の換算定数を用いて前記送信データを第 2 の代替値へ暗号化する暗号化処理と、前記第 1 の代替値、前記第 1 の換算定数、及び前記第 3 の換算定数又は前記第 4 の換算定数に対応するパターン換算定数を含む第 1 信号を生成する第 1 信号生成処理と、前記第 2 の代替値、前記第 2 の換算定数、及び前記第 1 信号に含まれない前記第 3 の換算定数又は前記第 4 の換算定数のパターン換算定数を含む第 2 信号を生成する第 2 信号生成処理と、を行う制御部と、前記第 1 信号と前記第 2 信号を外部へ送信する送信部と、を備える装置により実現できる。

【0038】

また、請求項 24 に記載のように、本発明は、送信データの暗号化に用いられる換算定数に対応するパターン換算定数を含む信号を転送する装置であって、前記換算定数に対応するパターン換算定数を記憶する記憶部と、前記信号を送受信する送受信部と、受信した前記信号に含まれるパターン換算定数を対応する前記換算定数に変換して前記信号を変換する信号生成処理と、前記変換された信号を

転送する処理と、を行う制御部と、を備える装置により実現できる。

【0039】

また、請求項25に記載のように、本発明は、第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを含む第1信号と第2'信号を受信して送信データを復号化する装置であって、前記第1信号には、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第1の代替値と、第1の換算定数と、が含まれ、前記第2'信号には、前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第2の代替値と、前記第2の換算定数と、前記第3の換算定数と、が含まれ、前記第1信号及び前記第2'信号を受信する受信部と、受信した前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数及び前記第3の換算定数を読取る処理と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化処理と、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2'信号を受け入れる認証をする認証処理と、を行う制御部と、を備える装置により実現できる。

【0040】

また、請求項26に記載のように、本発明は、第1の換算定数、第2の換算定数、第3の換算定数及び第4の換算定数のうち二の換算定数によって暗号化された送信データを含む第1'信号と第2'信号を受信して送信データを復号する装置であって、前記第1'信号には、前記第2の換算定数及び前記第4の換算定数を用いて前記送信データが暗号化された第1の代替値と、前記第1の換算定数と、前記第3の換算定数又は前記第4の換算定数と、が含まれ、前記第2'信号には、第1の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第1の代替値と、第2の換算定数と、前記第1'信号に含まれていない第3の換算定数又は前記第4の換算定数と、が含まれ、前記第1'信号及び前記第2'信号を受信する受信部と、受信した前記第1'信号から前記第1の代替値、前

記第1の換算定数、及び前記第3の換算定数又は第4の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数又は第4の換算定数を読取る処理と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化処理と、前記第1の複合化データと前記第2の復号化データから前記第1'信号及び前記第2'信号を受け入れる認証をする認証処理と、を行う制御部を備える装置により実現できる。

【0041】

また、請求項27に記載のように、本発明は、第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを含む第1信号と第2信号を受信して送信データを復号化する装置であって、前記第1信号には、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第1の代替値と、第1の換算定数と、が含まれ、前記第2信号には、前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第2の代替値と、前記第2の換算定数と、前記第3の換算定数に対応するパターン換算定数と、が含まれ、前記換算定数に対応するパターン換算定数を記憶する記憶部と、前記第1信号及び前記第2信号を受信する受信部と、前記第1信号から前記第1の代替値、及び前記第1の換算定数、前記第2信号から前記第2の代替値、前記第2の換算定数、及び前記パターン換算定数を読取る処理と、前記読取られたパターン換算定数から前記第3の換算定数を取得する処理と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化処理と、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2信号を受け入れる認証をする認証処理と、を行う制御部と、を備える装置により実現できる。

【0042】

また、請求項28に記載のように、前記制御部は、前記第1の復号化データ又は第2の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出するように構成することができる。

【0043】

また、請求項 29 に記載のように、前記制御部は、前記第 1 の複合化データと前記第 2 の復号化データが一致したときに前記認証を行うように構成することができる。

【0044】

【発明の実施の形態】

本発明の実施の形態について図面を参照して説明する。図 1 は第 1 のデータ送信方法の説明図、図 2 は第 2 のデータ送信方法の説明図である。図 3 は実施例のデータ送信システムの説明図、図 4 は実施例のデータ送受信側装置の構成図、図 5 は実施例の送信データの暗号化についての説明図、図 6 は実施例の第 1 信号の構成を表す説明図、図 7 は実施例の第 2 信号の構成を表す説明図である。

【0045】

図 8 は実施例の送信側装置のパターン換算定数データの説明図、図 9 は実施例の中継装置のパターン換算定数データの説明図、図 10 は実施例の第 2 信号の構成を表す説明図、図 11 は実施例の送信信号の復号化についての説明図、図 12 は実施例の送信信号の復号化についてのデータ例を示す説明図、図 13 は実施例の送信側装置の処理の流れを示す説明図、図 14 は実施例の中継装置の処理の流れを示す説明図、図 15 及び図 16 は実施例の受信側装置の処理の流れを示す説明図である。

【0046】

図 17 は第 1 のデータ送信方法の変形例を表す説明図、図 18 は第 1 のデータ送信方法の変形例を表す説明図である。図 19 は別実施例のデータ送信システムの説明図、図 20 は別実施例のデータ送信システムの構成装置の構成図、図 21 は別実施例の第 1 信号の構成を表す説明図、図 22 は別実施例の第 2 信号の構成を表す説明図である。また、以下に説明する配置、形状等は、本発明を限定するものではなく、本発明の趣旨に沿って各種改変することができることは勿論である。

【0047】

図 1 に基づき本発明のデータ送信システムに関する第 1 のデータ送信方法につ

いて説明する。本データ送信方法では、送信者（送信側装置）から受信者（受信側装置）へ、第1信号 S_1 と第2信号 S_2 が別々のルートで送信される。本発明の送信には、有線・無線回線を介した送信（例えば、赤外線通信、無線電波、光通信等による送信）及び伝送手段によるデータ等の送信（例えば、郵便等による配送）を含むものである。

【0048】

まず、送信側装置では、暗号鍵となる換算定数 X 、 Y とパターン換算定数 Z が選択される。なお、送信側装置及び中継装置には、パターン換算定数 Z に対して換算定数 Z' が関連付けて登録されている。送信側装置及び中継装置では、パターン換算定数 Z が選択されると、これに対応して換算定数 Z' が読み出される。

【0049】

送信側装置では、送信データ D は、換算定数 Y と Z' の組合せによって暗号化データ $D(Y, Z')$ に、換算定数 X と Z' の組合せによって暗号化データ $D(X, Z')$ に、それぞれ暗号化される。第1信号 S_1 には、暗号化データ $D(Y, Z')$ 、換算定数 X が含まれる。また、第2信号 S_2 には、暗号化データ $D(X, Z')$ 、換算定数 Y 、パターン換算定数 Z が含まれる。

【0050】

第1信号 S_1 は、受信側装置へ送信される。一方、第2信号 S_2 は、一旦、中継装置に送信される。そして、第2信号 S_2 は、中継装置で第2'信号 S_2' に変換される。すなわち、中継装置では、受信された第2信号 S_2 に含まれるパターン換算定数 Z が換算定数 Z' に変換される。そして、第2'信号 S_2' は、中継装置から受信側装置へ送信される。なお、第1信号 S_1 及び第2信号 S_2 は、送信側装置から時間をずらして送信されるようにしてもよい。

【0051】

受信側装置では、第1信号 S_1 及び第2'信号 S_2' を受信し、第1信号 S_1 から換算定数 X 、第2'信号 S_2' から換算定数 Y 、 Z' が読取られる。そして、第1信号 S_1 に含まれる暗号化データ $D(Y, Z')$ は、読取られた換算定数 Y と Z' の組合せによって復号化され、復号化データ D_1 が算出される。一方、第2'信号 S_2' に含まれる暗号化データ $D(X, Z')$ は、読取られた換算定

数 X と Z' の組合せによって復号化され、復号化データ D_2 が算出される。

【0052】

そして、復号化データ D_1 と D_2 との比較が行われる。受信側では両者が一致した場合に、復号化データ D_1 （又は D_2 ）を送信データ D として採用する。また、送信データ D には、受信側装置に接続された種々の外部駆動装置を駆動させるための駆動信号を含ませることができる。例えば、外部駆動装置としてのロックシステムを開閉操作することが可能となる。

【0053】

なお、上記暗号化例では、送信データ D を換算定数 Y と Z' の組合せ及び換算定数 X 、 Z' の組合せにより暗号化していたが、これに限らず、送信データ D を換算定数 Y と Z' の組合せによる暗号化（ $D(Y, Z')$ ）及び換算定数 X のみによる暗号化（ $D(X)$ ）をするようにしてもよい。この場合、第1信号 S_1 には暗号化データ $D(Y, Z')$ 、換算定数 X が含まれ、第2信号 S_2 には暗号化データ $D(X)$ 、換算定数 Y 、パターン換算定数 Z が含まれる。

【0054】

また、送信データ D を換算定数 Y のみによる暗号化（ $D(Y)$ ）、換算定数 X と Z' による暗号化（ $D(X, Z')$ ）をするようにし、第1信号 S_1 には暗号化データ $D(Y)$ 、換算定数 X が含まれ、第2信号 S_2 には暗号化データ $D(X, Z')$ 、換算定数 Y 、パターン換算定数 Z が含まれるようにすることもできる。

【0055】

このようにすれば、成りすまし送信された場合に、中継装置では不正な第2信号 S_2 に含まれるパターン換算定数 Z が、登録された対応関係により換算定数 Z' に変換される。そして、この対応関係が正しくない換算定数 Z' を含む第2'信号 S_2' が受信側へ転送される。

【0056】

しかし、この換算定数 Z' は成りすまし送信での暗号化に使用された換算定数とは異なるため、受信側で不正な第1信号 S_1 と不正な第2'信号 S_2' をもとに復号化すると、得られる復号化データ D_1 と D_2 が不一致となる。また、復号

化データは、有意なデータとして復号することはできない。

【0057】

以上のように第1のデータ送信方法では暗号化された送信データを2系統で送信する場合に、第1信号 S_1 に含まれる暗号化データの暗号鍵（換算定数 Y ）は第2信号 S_2 に含めて送信され、第2信号 S_2 に含まれる暗号化データの暗号鍵（換算定数 X ）は第1信号 S_1 に含めて送信される。

【0058】

さらに、第1信号 S_1 及び第2信号 S_2 に含まれる暗号化データの共通の暗号鍵（換算定数 Z' ）そのものは送付されず、暗号鍵に対応するパターン換算定数 Z が第2信号 S_2 に含めて中継装置へ送信される。そして、このパターン換算定数 Z が、中継装置で換算定数 Z' へ変換されることにより、第2信号 S_2 が第2'信号 S_2' に変換され、受信側へ転送される。

【0059】

このように送信することにより、第3者は第1信号 S_1 及び第2信号 S_2 の双方を取得したとしてもパターン換算定数 Z が不明であるので、送信データ D の復号化を行うことはできない。また、第3者が第1信号 S_1 又は第2'信号 S_2' の一方を取得したとしても、それぞれの信号には換算定数のすべての換算定数が含まれていないので、復号化を行うことはできない。

【0060】

さらに、第3者が第1信号 S_1 及び第2'信号 S_2' の双方を取得したとしても、復号化方法を取得しない限り、有意な復号化データを得ることはできない。

【0061】

以上のように、第1のデータ送信方法では、第3者が暗号化データを不正に取得したとしても、暗号化データの復号化を有意に行うことができず、送信データの秘匿性を高めることができる。

【0062】

また、受信側では、送信側で登録されたパターン換算定数を知らなくても暗号化データを復号化することができる。したがって、送信側では複数のパターン換算定数 Z 及び換算定数 Z' の組合せを登録することにより、複数の受信者（受信

側装置)へ暗号化データを送信する場合にも秘匿性を高めることができる。

【0063】

そして、第3者には換算定数 X 、 Y 、 Z' による暗号化方法及びパターン換算定数が不明であるため、送信者に成り代わって送信したとしても、受信側では有意なデータとして復号化することができない。または、復号化データが一致しない。これにより、成りすまし送信による不都合を回避することができる。

【0064】

次に、図2に基づき第2のデータ送信方法について説明する。送信者(送信側装置)から受信者(受信側装置)へ第1信号 S_1 と第2信号 S_2 が別々のルートで送信されるのは、第1のデータ送信方法と同様である。また、送信側装置から送信される第1信号 S_1 及び第2信号 S_2 についても、暗号化方法やそれぞれに含められる換算定数等は同様である。

【0065】

第2のデータ送信方法と上述の第1のデータ送信方法との違いは、第2信号 S_2 が中継装置を介して送信されないことである。そのため、第1のデータ送信方法では送信側と中継装置にパターン換算定数 Z 及び換算定数 Z' が登録されていたが、第2のデータ送信方法では送信側と受信側にパターン換算定数 Z 及び換算定数 Z' が登録されている。

【0066】

したがって、受信側装置では、第1信号 S_1 及び第2信号 S_2 が受信され、第1信号 S_1 から換算定数 X 、第2信号 S_2 から換算定数 Y 及びパターン換算定数 Z が読取られる。そして、受信側装置で読取られたパターン換算定数 Z に対応する換算定数 Z' が読み込まれる。

【0067】

これにより、第1信号 S_1 に含まれる暗号化データ $D(Y, Z')$ (又は $D(Y)$)は、換算定数 Y と Z' の組合せ(又は Y のみ)によって復号化データ D_1 に復号化され、第2信号 S_2 に含まれる暗号化データ $D(X, Z')$ (又は $D(X)$)は、換算定数 X と Z' の組合せ(又は X のみ)によって復号化データ D_2 に復号化される。

【0068】

または、第1信号 S_1 に含まれる暗号化データ $D(Y, Z')$ (又は $D(Y)$) は、換算定数 Y と Z' の組合せ (又は Y) によって復号化データ D_1 に復号化され、第2信号 S_2 に含まれる暗号化データ $D(X)$ (又は $D(X, Z')$) は、換算定数 X (又は X と Z' の組合せ) によって復号化データ D_2 に復号化される。

【0069】

そして、受信側では第1のデータ送信方法と同様に両者が一致した場合に、復号化データ D_1 (又は D_2) が送信データ D として採用される。

【0070】

以上のように第2のデータ送信方法では暗号化された送信データを2系統で送信する場合に、第1信号 S_1 に含まれる暗号化データの暗号鍵 (換算定数 Y) は第2信号 S_2 に含めて送信され、第2信号 S_2 に含まれる暗号化データの暗号鍵 (換算定数 X) は第1信号 S_1 に含めて送信される。これは、第1のデータ送信方法と同様である。

【0071】

そして、第1信号 S_1 及び第2信号 S_2 に含まれる暗号化データの共通の暗号鍵 (換算定数 Z') そのものは送付されず、暗号鍵に対応するパターン換算定数 Z が第2信号 S_2 に含めて送信される。

【0072】

そして、第2信号 S_2 を受信した受信側装置では、予め有しているパターン換算定数 Z と換算定数 Z' の組合せの登録データを参照して、第2信号 S_2 に含まれるパターン換算定数 Z から換算定数 Z' を読み込み、さらに第1信号 S_1 及び第2信号 S_2 から得られた換算定数 X, Y を使用して、送信データ D を復号化している。

【0073】

このように、送信側及び受信側に予めパターン換算定数を登録しておくことにより、送信側と受信側との一対一の秘匿データ送信が可能となる。このような、送信方法を利用して、例えば外部駆動装置としてのドアロックの開閉操作等を行

うことができる。漏洩データに対する復号化が困難であること、及び成りすまし送信による不都合を回避できることは、第1のデータ送信方法と同様である。

【0074】

なお、第1及び第2の送信方法では、換算定数 X 、 Y 、 Z の3つの暗号鍵を用いて暗号化しているが、換算定数 X 、 Y 、 Z は、それぞれ換算定数 X_1 、 X_2 、 \dots 、換算定数 Y_1 、 Y_2 、 \dots 、換算定数 Z_1 、 Z_2 、 \dots 、のようにそれぞれ複数の換算定数を含む概念である。また、例えば、換算定数 X に複数の換算定数(X_1 、 X_2 、 \dots)が用いられる場合は、これら複数の換算定数を第1信号 S_1 、第2信号 S_2 のどちらか、もしくは分散して両方に配置してもよい。

【0075】

次に、第1の送信方法を用いた実施例の概略を図3に基づいて説明する。本例のデータ送信システム S は、一方の送受信装置1（以下、「装置1」という）からインターネット I を介して他方の送受信装置1へ暗号化された送信データを送信するものである。

【0076】

第1信号 S_1 は、送信側の装置1からプロバイダ P を介して受信側の装置1のアドレスへ向けて送信され、受信側の装置1は第1信号 S_1 を受信する。また、第2信号 S_2 は、送信側の装置1からプロバイダ P を介して中継配信サーバプロバイダ2（以下、「中継装置2」という）へ向けて送信される。中継装置2では、第2信号 S_2 を第2'信号 S_2' に変換して、これを受信側の装置1のアドレスへ向けて送信する。受信側の装置1は、第2'信号 S_2' を受信する。

【0077】

本例のデータ送信システム S では、送信データとして個人認証番号 A 、搬送認証番号 B 、制御データ C 、機密データ D_t が送信される。個人認証番号 A 、搬送認証番号 B 、制御データ C は、第1乃至第3の換算定数としての換算定数 X 、 Y 、 $Z_{y'}$ で暗号化され、第1信号 S_1 及び第2信号 S_2 に含められる。また、機密データ D_t は別途秘匿化されて第1信号 S_1 に含められる。

【0078】

受信側の装置 1 では、第 1 信号 S_1 及び第 2' 信号 S_2' を受信して、両信号から換算定数 X , Y , Z_y' を読取り、これらにより両信号に含まれる暗号化された個人認証番号 A , 搬送認証番号 B , 制御データ C に関するデータを復号し、また、機密データ D_t の復号化を行う。さらに、復号化された制御データ C に基づき、外部装置が駆動される。

【0079】

本例の換算定数 X , Y は、乱数によって装置 1 内で生成される。したがって、送信毎に異なる換算定数が選択されるものである。また、送信側の装置 1 は、特有のパターン換算定数データを有しており、パターン換算定数データには、パターン換算定数 Z_y と換算定数 Z_y' の複数の組合せ（本例では、26 通り）が送信者により登録されている。なお、このパターン換算定数データは、中継装置 2 にも送信者毎に対応して登録されている。

【0080】

本システム S に登録された送信者は、固有の個人認証番号 A を有しており、装置 1 を用いて個人認証番号 A , 搬送認証番号 B , 制御データ C , 機密データ D_t を送信することができる。受信者は、送信者から送られてきた 2 つの信号を受信し、これらから装置 1 によって送信データの認証を行い、個人認証番号 A , 搬送認証番号 B , 制御データ C , 機密データ D_t を取得することができる。

【0081】

搬送認証番号 B は、送信者が商品の搬送認証番号等を受信者に送付するためのものであり、売り手側から買い手側へ商品等を受け渡す流通手段として、又は受け渡しロッカー等の用途に使用することができる。また、クレジットカード番号の送信にも使用することができる。

【0082】

制御データ C は、送信側から受信側へ販売金額、利用回数、バーコード出力、リモート制御の ON/OFF 信号、鍵の解錠/施錠信号等の制御信号を送付するためのものである。

【0083】

機密データ D_t は、送信者が受信者へ見積書、医療カルテ、法文書、成績書そ

の他の機密文書等を封印して送信するためのものである。機密データ D_t は別途秘匿化されて第1信号 S_1 に含まれる。

【0084】

中継装置2には、上述のように複数の登録送信者ごとのパターン換算定数データが記憶されており、各登録送信者からの第2信号 S_2 を受信して、該信号中のパターン換算定数を該当する換算定数へ変換して第2'信号 S_2' を生成し、第2信号 S_2 に付随して送信されてきた受信者のアドレスへ転送している。

【0085】

また、中継装置2は、このようなデータ管理、データ変換及びデータ転送等の処理を行うと共に、データ転送等の処理に基づいて課金を行うための課金データ作成処理を行う。これにより、各登録送信者に対して、利用に応じて利用料の請求を行うことができる。このような課金については、利用回数、データ量等に応じて行うことが考えられる。

【0086】

次に、図4に基づいて装置1及び中継装置2の構成について説明する。装置1は、専用機として構成してもよいが、通常のデスクトップ型のパソコンやモバイル端末を使用した構成としてもよい。装置1は、制御部としてのCPU100と、データの入出力を行うための入出力部101と、データの表示を行うための表示部102と、送受信部103と、各種データが記憶された記憶部110と、を備えている。

【0087】

CPU100は、データの入出力制御、データ送受信制御、データの暗号化及び復号化処理、データ読取処理、第1信号及び第2信号の生成処理、認証処理、外部駆動装置の制御等を行う。データの暗号化処理については、CPU100は、乱数によって換算定数を自動選択（換算定数選択処理）し、該換算定数による所定の暗号化式にしたがって暗号化手段として入力データの暗号化（暗号化処理）を行う。なお、換算定数は送信者が指定して、該換算定数がCPU100に選択されるようにしてもよい。

【0088】

入出力部 101 は、送信データとしての個人認証番号 A、搬送認証番号 B 等や受信者のアドレス入力、パターン換算定数データ登録、データ暗号化・復号化处理、バーコードの読取処理等に用いられるものであり、例えばキーボード、マウス、バーコードリーダー、各種記憶メディアとのデータ入出力装置等から構成される。

【0089】

表示部 102 は、入出力データ等の表示を行うものであり、例えば LCD 装置等から構成される。送受信部 103 は、インターネット I 及び外部駆動装置等に接続され、外部とデータの送受信を行うものであり、例えばモデムや LAN カード等である。

【0090】

記憶部 110 は、主記憶部 111 と、ROM 112 と、RAM 113 とを備える。主記憶部 111 には、オペレーティングシステムプログラムや、本例のデータ送受信処理等を行うためのプログラムを含む各種アプリケーションプログラム、パターン換算定数データ 111a 等が記憶されている。また、ROM 112 には、基本プログラム等が記憶され、ROM 113 は作業エリアとして用いられる。

【0091】

送信者は、データ送信時にデータ送信システム S 用の制御プログラムを起動して装置 1 の入出力部 101 から所定のデータの入力操作及びその他の送信操作を行う。また、受信者は、信号を受信して復号操作等を行う。

【0092】

また、本例の中継装置 2 は、プロバイダ内に配設されるサーバコンピュータとして実現することができる。中継装置 2 は、制御部としての CPU 200、入出力部 201、表示部 202、送受信部 203、記憶部 210 とを備えている。記憶部 210 は、主記憶部 211、ROM 212、RAM 213 を備えている。また、主記憶部 211 内には、上述した登録者毎のパターン換算定数データ 211a が記憶されている。CPU 200 は、信号の送受信処理、データ読取処理、信号の変換処理（信号生成処理）等を行う。

【0093】

次に、図5に基づき送信データの暗号化について説明する。上述のように本例の暗号化には乱数によって生成される換算定数 X 、 Y 、及び送信者が選択するパターン換算定数 Z_y に対応する換算定数 Z_y' が用いられる。なお、パターン換算定数 Z_y は送信者が選択するのではなく、暗号化時に登録されたパターン換算定数データから自動的に選択されるように構成してもよい。

【0094】

図5に示すように、個人認証番号 A は第1式($A_x = A + Y + Z_y'$)及び第2式($A_y = A + X + Z_y'$)、搬送認証番号 B は第1式($B_x = B + Y + Z_y'$)及び第2式($B_y = B + X + Z_y'$)、制御データ C は第1式($C_x = C + Y + Z_y'$)及び第2式($C_y = C + X + Z_y'$)にしたがい暗号化される。それぞれのデータは、個人ID代替値(A_x , A_y)、搬送ID代替値(B_x , B_y)、制御データ代替値(C_x , C_y)に暗号化される。

【0095】

例えば、図5に示したように、個人認証番号 A を「123456789012」, 搬送認証番号 B を「031234567890」, 制御データ C を「20000」, 換算定数 X を「223344」, 換算定数 Y を「445566」, 換算定数 Z を「3399」とすると、それぞれのデータは第1式及び第2式によって、個人認証番号 A は「123457237977」, 「123457015755」、搬送認証番号 B は「031235016855」, 「031234794633」、制御データ C は「468965」, 「246743」に暗号化される。

【0096】

本例の暗号化は、図5に示したように送信データに換算定数 X と Z_y' , 換算定数 Y と Z_y' がそれぞれ加算されるものであるが、これに限らず、減算, その他の演算方法であってもよい。また、上述したように送信データに換算定数 X と Z' , 換算定数 Y のみによって演算する方法、又は、送信データに換算定数 X のみ, 換算定数 Y と Z' によって演算する方法により暗号化してもよい。

【0097】

例えば、送信データに換算定数 X のみ、換算定数 Y と Z' による加算を行う場合は、個人認証番号 A は第1式($A_x = A + Y + Z_y'$)及び第2式($A_y = A + X$)、搬送認証番号 B は第1式($B_x = B + Y + Z_y'$)及び第2式($B_y = B + X$)、制御データ C は第1式($C_x = C + Y + Z_y'$)及び第2式($C_y = C + X$)にしたがい暗号化される。このようにすると、より成りすまし送信に対する不都合を排除する効果を向上させることができる。

【0098】

次に、図6及び図7に基づき第1信号 S_1 及び第2信号 S_2 について説明する。第1信号 S_1 及び第2信号 S_2 は、それぞれ大きさが指定されたパケット1乃至パケット10の10のデータ領域からなる。パケット0は、第1信号 S_1 及び第2信号 S_2 の内容を作成する際に入力するパスワードを一時的に格納するための領域であって、実際にデータとしては送信されないものである。

【0099】

パケット1は、通信番号格納領域であって送信信号に対して自動的に生起される番号である。パケット2は、送信者アドレス格納領域であって送信者の電子メールアドレスが入力される。パケット3は、送信者の登録名の格納領域である。

【0100】

パケット4は、第1信号 S_1 の場合は換算定数 X が、第2信号 S_2 の場合は換算定数 Y が格納される領域である。パケット5は、パターン換算定数 Z_y の格納領域である。本例の場合、パターン換算定数 Z_y は第1信号 S_1 には入力されず、第2信号 S_2 のみに入力される。図7の例では、パターン換算定数 Z_y として「g」が選択されている。パターン換算定数 Z_y の「g」は、換算定数 Z の「3399」に対応している。

【0101】

パケット6は、第1信号 S_1 、第2信号 S_2 において、個人認証番号 A がそれぞれ第1式、第2式によって暗号化された個人ID代替値 A_x 、 A_y が格納される領域である。同様にパケット7は、搬送認証番号 B がそれぞれ第1式、第2式によって暗号化された搬送ID代替値 B_x 、 B_y が格納される領域である。また、パケット8は、制御データ C がそれぞれ第1式、第2式によって暗号化された

制御データ代替値 C_x , C_y が格納される領域である。

【0102】

パケット 9 は、制御パターン C_p が格納される領域である。制御パターン C_p とは、制御データ C の制御パターンを指定するものであり、例えば制御パターン C_p が a の場合は、制御データ C は回数を意味するものであることを表す。

【0103】

同様に制御パターン C_p が、 b , c , d , e のときは、それぞれ制御データ C は、プリペイド金額・販売金額等の金額データ、数値・バーコード出力等の数値データ、リモート制御のための ON/OFF 信号データ、ロックシステムの解錠／施錠信号データを意味するものであることを表す。本例の場合、制御パターン C_p は第 1 信号 S_1 のみに格納される。図 6 の例では、制御パターン C_p として「 b 」が選択されている。

【0104】

また、パケット 10 は、機密データ D_t が格納される領域である。本例の場合、機密データ D_t は第 1 信号 S_1 のみに格納される。以上のような第 1 信号 S_1 及び第 2 信号 S_2 は、電子メールに添付されるデータファイルの形式で送信することができる。なお、制御パターン C_p , 機密データ D_t は、第 2 信号 S_2 に配置されてもよい。

【0105】

図 8 に示すように、装置 1 内に記憶されるパターン換算定数データ $111a$ は、パターン換算定数 $Z(a, b, \dots)$ にそれぞれ対応して換算定数 $Z_{y'}$ ($1234, 2345, \dots$) が関係付けられたものである。登録送信者は、装置 1 に自らが指定した 26 の換算定数 $Z_{y'}$ を登録することができる。また、データ送信システム S の管理者を介して、又は、直接、中継装置 2 に自ら指定したパターン換算定数データ $111a$ を登録することができる。

【0106】

図 9 に示すように、中継装置 2 内に登録されるパターン換算定数データ $211a$ は、複数の登録送信者のパターン換算定数データ $111a$ から構成されている。登録送信者ごとのパターン換算定数データ $111a$ は、各登録送信者の電子メ

ールアドレス及び送信者の登録名によって区別されている。

【0107】

次に、図10に基づき第2'信号 S_2' について説明する。送信側の装置1からの第2信号 S_2 は、プロバイダP経由で中継装置2へ一旦送信される。中継装置2では、上述のように第2信号 S_2 から第2'信号 S_2' に変換される。

【0108】

中継装置2では、第2信号 S_2 のパケット2（送信者アドレス）及びパケット3（登録名）を参照して、パターン換算定数データ211aから送信者のパターン換算定数データ111aが選択される。そして、選択されたパターン換算定数データ111aから第2信号 S_2 のパケット5（パターン換算定数 Z_y ）を参照して、これに対応する換算定数 $Z_{y'}$ が特定される。

【0109】

換算定数 $Z_{y'}$ が特定されると、第2信号 S_2 のパケット5が、特定されたパターン換算定数 $Z_{y'}$ の値に変換された第2'信号 S_2' が生成される。このように、中継装置2では、受信された第2信号 S_2 が第2'信号 S_2' に変換される。そして、第2'信号 S_2' は、送信者が指定する受信者の電子メールアドレスへ転送される。図10の例では、第2'信号 S_2' のパケット5（パターン換算定数格納領域）は「g」から「3399」へ変換される。

【0110】

次に、図11に基づき受信側の装置1で行われる復号化処理の概略について説明する。受信側の装置1で第1信号 S_1 及び第2'信号 S_2' が受信されると、両信号がペアリングされて仮認証される。このとき、通信番号、発信者アドレス等の一致が確認される。仮認証の結果、両信号が同一送信者からの受信信号であることが確認されると、両信号の暗号化データの復号化処理が行われる。

【0111】

まず、復号化処理では、両信号から換算定数 X 、 Y 、 $Z_{y'}$ が特定される。次に、個人ID代替値を復号化するための第1式（ $A_1 = A_x - Y - Z_{y'}$ ）及び第2式（ $A_2 = A_y - Y - Z_{y'}$ ）によってそれぞれ第1信号 S_1 の個人ID代替値 A_x 、第2'信号 S_2' の個人ID代替値 A_y が復号化される。

【0112】

そして、第1信号 S_1 及び第2'信号 S_2' のパケット3の送信者の登録名が一致すること、及び、復号化されたデータ(A_1 , A_2)が一致することが確認される。登録名及び復号化データ A_1 と A_2 が一致すれば、両信号が最終的に認証される。

【0113】

なお、個人ID代替値を復号化するための第1式が $A_1 = A_x - Y - Z_{y'}$ であり、第2式が $A_2 = A_y - Y$ である場合も同様に個人ID代替値 A_x , A_y が復号化されて復号化データ A_1 及び A_2 が算出され、登録名及び復号化データ A_1 及び A_2 の比較が行われ、両者が一致すれば、両信号が最終的に認証される。

【0114】

また、最終的に認証されると、搬送ID代替値を復号化するための第1式($B_1 = B_x - Y - Z_{y'}$)及び第2式($B_2 = B_y - Y - Z_{y'}$)によってそれぞれ第1信号 S_1 の搬送ID代替値 B_x , 第2'信号 S_2' の搬送ID代替値 B_y が復号化され、復号化データ B_1 と B_2 が一致すれば、搬送認証番号 B として復号化データ B_1 (又は B_2)が採用される。

【0115】

また、同様に、制御データ代替値を復号化するための第1式($C_1 = C_x - Y - Z_{y'}$)及び第2式($C_2 = C_y - Y - Z_{y'}$)によってそれぞれ第1信号 S_1 の制御データ代替値 C_x , 第2'信号 S_2' の制御データ代替値 C_y が復号化され、復号化データ C_1 と C_2 が一致すれば、制御データ C として復号化データ C_1 (又は C_2)が採用される。

【0116】

搬送ID代替値を復号化するための第1式が $B_1 = B_x - Y - Z_{y'}$ 、第2式が $B_2 = B_y - Y$ であり、制御データ代替値を復号化するための第1式が $C_1 = C_x - Y - Z_{y'}$ 、第2式が $C_2 = C_y - Y - Z_{y'}$ である場合も同様である。

【0117】

また、制御パターン C_p により、制御データ C の種類が特定される。さらに、制御データ C の種類が、外部駆動装置へのON/OFF信号データ、解錠/施錠

信号データであった場合は、受信側の装置 1 からさらに外部装置へ該信号が送出され、外部駆動装置が駆動されるようになっている。

【0118】

図 12 に示すように、両信号の登録名が「xxxxxx」であるので、登録名(Nm)は一致する。そして、個人ID代替値Axとして「123457237977」、個人ID代替値Ayとして「123457015755」を受信していた場合、換算定数X、Y、Zy'を所定の packets から読み出して復号化が行われると、図 12 の場合、復号化データA₁及びA₂は共に「123456789012」となり両者は一致するため、両信号は正規のものであるとの最終認証が行われる。

【0119】

また、搬送ID代替値Bx、Byがそれぞれ「031235016855」, 「031234794633」であった場合は、復号化データB₁とB₂が共に「031234567890」となるので両者は一致する。

【0120】

また、制御データ代替値Cx、Cyがそれぞれ「468965」, 「246743」であった場合は、復号化データC₁とC₂が共に「20000」となるので両者は一致する。これにより、搬送認証番号B、制御データCには、それぞれ「031234567890」, 「20000」が採用される。

【0121】

次に、図 13 に基づき送信側の装置 1 のデータ処理の流れについて説明する。まず、ステップS10では、画面表示に従って送信者が入力した所定のデータが読み込まれる。所定の入力データとしては、第1信号S₁及び第2信号S₂に関連したものとして、送信者の電子メールアドレス(packets 2)、送信者名(登録名、packets 3)、パターン換算定数Zy(packets 5)、個人認証番号A、搬送認証番号B、制御データC、制御パターンCp(packets 9)、機密データDt、また、他のデータとして受信者の電子メールアドレス、中継装置 2 の電子メールアドレス等がある。

【0122】

なお、パスワード（パケット 0）を入力するようにして、登録送信者以外の者が装置 1 を用いて送信操作できないように制限をかけるようにしてもよい。

【0123】

次にステップ S 1 1 では、データ入力（S 1 0）されたタイミングで選択された 2 つの乱数（本例の場合 6 桁の数）を換算定数 X 、 Y とし、また、ステップ S 1 0 で入力されたパターン換算定数 Z_y に対応する換算定数 $Z_{y'}$ をパターン換算定数データ 1 1 1 a から読み出す。

【0124】

そして、ステップ S 1 2 へ進み、ステップ S 1 0 で入力された個人認証番号 A 、搬送認証番号 B 、制御データ C を換算定数 X 、 Y 、 $Z_{y'}$ によって暗号化し、また、別途機密データ D_t を暗号化する。機密データ D_t の暗号化手法については、個人認証番号 A 、制御データ C や換算定数 $Z_{y'}$ 等を暗号鍵として暗号化してもよい。

【0125】

ステップ S 1 3 では、ステップ S 1 2 で暗号化されたデータ及びステップ S 1 0 で入力された入力データに基づき、所定の大きさを有する格納領域に各データを配置することにより第 1 信号 S_1 が生成される。

【0126】

次にステップ S 1 4 では、ステップ S 1 3 と同様に第 2 信号 S_2 が生成される。ステップ S 1 3 及び S 1 4 では、例えば第 1 信号 S_1 のパケット 5 のように配置すべきデータがない場合には、ブランクデータもしくは所定のスクランブルデータが配置される。

【0127】

また、例えば搬送認証番号 B は送信するが、制御データ C は送信する必要がない場合、制御データ C にはステップ S 1 0 でブランクデータが入力される。この場合も、ブランクデータ（又はスクランブルデータ）を入力データとして、ステップ S 1 3 及び S 1 4 でデータが生成される。

【0128】

そして、ステップ S 1 5 では、送信者の送信入力に基づいて、先ず指定された

受信者のアドレスへ第1信号 S_1 が送信される。次いでステップS16で、指定された中継装置2のアドレスへ第2信号 S_2 が送信され、処理を終了する。

【0129】

次に、図14に基づき中継装置2での処理の流れについて説明する。中継装置2は、ステップS20で所定の電子メールアドレスに送信者からの第2信号 S_2 が送信されてくるのを待ち、ステップS20で第2信号 S_2 を受信すると（ステップS20；Yes）、ステップS21へ進み、送信者の識別を行う。

【0130】

ステップS21では、受信した第2信号 S_2 の送信者の電子メールアドレス（パケット2）及び登録名（パケット3）を読み込む。そして、ステップS22で、該電子メールアドレス及び登録名がパターン換算定数データ211aに登録されているか否かを判別する。

【0131】

ステップS22で該電子メールアドレス及び登録名が登録されていれば（ステップS22；Yes）、パターン換算定数データ111aを特定してステップS23へ進む。一方、登録されていなければ（ステップS22；No）、正規の登録送信者からの信号でないと判断して処理を終了する。なお、このとき、受信者へ不正な第2信号 S_2 を受信した旨の電子メールを送信するようにしてもよい。

【0132】

ステップ23では、第2信号 S_2 のパターン換算定数 Z_y （パケット5）を読取る。ステップS24では、ステップS22で特定されたパターン換算定数データ111aを参照して、読取られたパターン換算定数 Z_y に対応する換算定数 $Z_{y'}$ を読取る。

【0133】

そして、ステップS25で、ステップS24で読取られた換算定数 $Z_{y'}$ を用いて第2'信号 $S_{2'}$ を生成する。ステップS26では、ステップS25で生成された第2'信号 $S_{2'}$ を、第2信号 S_2 と共に送付されてきた受信者の電子メールアドレスに送信し、処理を終了する。

【0134】

次に、図15及び図16に基づき、受信側の装置1の処理の流れについて説明する。ステップS30で、第1信号 S_1 及び第2'信号 S_2' を受信して装置1内に取り込む。そして、装置1に取り込まれた第1信号 S_1 及び第2'信号 S_2' が受信者によって一对の信号であると指定される。具体的には、受信者が受取った電子メールに添付されたデータファイルが、装置1の画面上で第1信号 S_1 及び第2'信号 S_2' に指定される。

【0135】

ステップS32では、指定された2つの信号の通信番号（パケット1）に相当するデータが比較される。両信号の通信番号が一致した場合は（ステップS32；Yes）、ステップS33へ進む。一方、両信号の通信番号が一致しなかった場合は（ステップS32；No）、ステップS48へ進み、表示部102にその旨のエラー表示をして処理を終了する。

【0136】

ステップS33では、第1信号 S_1 のパケット3乃至パケット10のデータが読取られる。また、ステップS34では、第2'信号 S_2' のパケット3乃至パケット10のデータが読取られる。

【0137】

次にステップS35では、個人ID代替値 A_x を復号化するための第1式から復号化データ A_1 が算出される。ステップS36では、個人ID代替値 A_y を復号化するための第2式から復号化データ A_2 が算出される。そして、ステップS37でステップS33及びS34で読取られた登録名、復号化データ A_1 と A_2 がそれぞれ比較され、一致するか否かが判別される。

【0138】

これらが一致すると（ステップS37；Yes）、ステップS38へ進む。一方、一致しなかった場合は（ステップS37；No）、ステップS49へ進み、登録名、復号化データ A_1 と A_2 が一致しない旨のエラー表示をして処理を終了する。一致しない場合としては、成りすまし送信で暗号化式が不正であった場合、成りすまし送信でパターン換算定数 Z_y と換算定数 $Z_{y'}$ との対応関係の不一致の場合等である。

【0139】

ステップS38では、搬送ID代替値 B_x を復号化するための第1式から復号化データ B_1 が算出される。ステップS39では、搬送ID代替値 B_y を復号化するための第2式から復号化データ B_2 が算出される。そして、ステップS40で復号化データ B_1 と B_2 が比較され、一致するか否かが判別される。

【0140】

これらが一致すると（ステップS40；Yes）、ステップS41へ進む。一方、一致しなかった場合は（ステップS40；No）、ステップS50へ進み、復号化データ B_1 と B_2 が一致しない旨のエラー表示をして処理を終了する。

【0141】

ステップS41では、制御データ代替値 C_x を復号化するための第1式から復号化データ C_1 が算出される。ステップS42では、制御データ代替値 C_y を復号化するための第2式から復号化データ C_2 が算出される。そして、ステップS43で復号化データ C_1 と C_2 が比較され、一致するか否かが判別される。

【0142】

これらが一致すると（ステップS43；Yes）、ステップS44へ進む。一方、一致しなかった場合は（ステップS43；No）、ステップS51へ進み、復号化データ C_1 と C_2 が一致しない旨のエラー表示をして処理を終了する。

【0143】

ステップS44では、機密データ D_t の復号がなされる。ステップS45では、復号化データ A_1 、 B_1 、 C_1 をそれぞれ、個人認証番号A、搬送認証番号B、制御データC、機密データ D_t として表示部102に表示する。また、制御パターン C_p により、制御データCの種類が表示される。なお、機密データ D_t は、受信者によって手動で表示画面上において2つの受信信号が指定（例えば、両信号のデータファイルを重ね合わせる等）され、かつ復号データ A_1 と A_2 が一致することを条件に、封印から開封（復号）されるように構成することができる。

【0144】

ステップS46では、制御パターン C_p により制御データCが外部駆動装置を

駆動する信号であるか否かが判別される。制御データ C が外部駆動信号データであった場合は（ステップ S 4 6 ; Y e s）、ステップ S 4 7 へ進み、所定の外部駆動装置へ駆動信号を送出し、処理を終了する。一方、制御データ C が外部駆動信号データでなかった場合は（ステップ S 4 6 ; N o）、処理を終了する。

【0145】

なお、上記実施例（第 1 のデータ送信方法）では、第 1 信号 S_1 はプロバイダ P を介して直接、送信側の装置 1 から受信側の装置 1 へ送信されるが、第 2 信号 S_2 は中継装置 2 を介して第 2' 信号 S_2' に変換されて受信側の装置 1 へ送信される。しかし、図 17 に示すように第 2 信号 S_2 だけでなく、第 1 信号 S_1 も別の中継装置 2 を介して受信側の装置 1 へ送信するようにしてもよい。

【0146】

この場合、パターン換算定数データは、送信側の装置 1 及び 2 つの中継装置 2 に登録される。そして、送信側の装置 1 及び 2 つの中継装置 2 では、乱数により選択される換算定数 X 、 Y と、パターン換算定数 Z_x 、 Z_y を指定することによりそれぞれ特定される換算定数 Z_x' 、 Z_y' の 4 つの換算定数が暗号鍵として用いられる。

【0147】

送信側の装置 1 では、送信データ D が換算定数 Y 、 Z_y' により暗号化データ $D(Y, Z_y')$ に暗号化され（例えば、 $D(Y, Z_y') = D + Y + Z_y'$ ）、また、換算定数 X 、 Z_x' により暗号化データ $D(X, Z_x')$ に暗号化される（例えば、 $D(X, Z_x') = D + X + Z_x'$ ）。

【0148】

そして、第 1 信号 S_1 には、暗号化データ $D(Y, Z_y')$ 、換算定数 X とパターン換算定数 Z_x が含まれる。また、第 2 信号 S_2 には、暗号化データ $D(X, Z_x')$ 、換算定数 Y とパターン換算定数 Z_y が含まれる。これら両信号は、送信側の装置 1 からそれぞれ第 1 の中継装置 2、第 2 の中継装置 2 へ送信される。

【0149】

第 1 の中継装置 2 では、第 1 信号 S_1 のうちのパターン換算定数 Z_x が換算定

数 Z_x' に変換されて第 1' 信号 S_1' が生成され、第 1' 信号 S_1' は受信側の装置 1 のアドレスへ転送される。また、第 2 の中継装置 2 では、第 2 信号 S_2 のうちパターン換算定数 Z_y が換算定数 Z_y' に変換されて第 2' 信号 S_2' が生成され、第 2' 信号 S_2' は受信側の装置 1 のアドレスへ転送される。

【0150】

受信側の装置 1 では、第 1' 信号 S_1' から換算定数 X , Z_x が読取られ、第 2' 信号 S_2' から換算定数 Y , Z_y が読取られる。読取られた換算定数 X , Y , Z_x , Z_y によって、第 1' 信号 S_1' 及び第 2' 信号 S_2' は、それぞれ復号化データ D_1 及び D_2 に復号化される。そして、受信側の装置 1 では、復号化データ D_1 と D_2 の比較認証が行われ、両者が一致すれば復号化データ D_1 (又は D_2) が送信データ D として採用される。

【0151】

このように、2 つの送信信号にそれぞれ異なる換算定数 Z_x , Z_y を用いて暗号化された暗号化データが含まれ、また、2 つの送信信号には暗号化に用いられた換算定数ではない換算定数に対応するパターン換算定数が含まれる。そして、2 つの送信信号は、別々のルートを通して別々の中継装置 2 に一旦、送信され、中継装置 2 で送信信号に含まれたパターン換算定数が換算定数に変換され、それぞれ変換された送信信号が受信側の装置 1 に転送される。

【0152】

このように、2 ルート共に中継装置 2 を介して送信信号を変換・転送することにより、よりデータの秘匿性を高めることができ、成りすまし送信等の不正行為を確実に防止することができる。

【0153】

また、上記実施例では、第 1 信号 S_1 及び第 2 信号 S_2 の双方がインターネット I 経由で送信側から受信側へ送信されていたが、これに限らず、図 18 に示すようにバーコード出力された第 1 信号 S_1 を搬送商品に添付して送付し、第 2 信号 S_2 は中継装置 2 を介してインターネット I 経由で受信側へ送信する利用形態も可能である。

【0154】

第1信号S₁はバーコードリーダーによって受信側の装置1に取り込まれ、第2'信号S₂'はインターネットI経由で受信される。これら両信号により搬送認証番号B等を復号化し、認証を行うことができる。

【0155】

次に、図19に基づき第2のデータ送信方法による実施例を説明する。本実施例では、リモート制御により電子錠を解錠／施錠するロックシステムS-2に適用した例について説明する。本システムS-2は、第1信号S₁及び第2信号S₂を送信する装置3と、両信号を受信して外部駆動装置を駆動操作する装置4と、外部駆動装置としての電子錠5によって構成される。なお、第2のデータ送信方法は、例えばパソコン等の個人認証に適用することも可能である。

【0156】

装置3は、カード型の薄型小型装置であって、赤外線によって装置4へ第1信号S₁及び第2信号S₂を送信する。また、装置4は、赤外線受光部で該赤外線信号を受信して、該信号を認証後、外部駆動装置である電子錠5へ開閉駆動信号を送出する。電子錠5は、解錠／施錠駆動信号を受けるとこれに従い、電子ロックの解錠又は施錠操作を行う。

【0157】

図20に基づき本システムS-2の装置3及び装置4の構成を説明する。装置3は、制御部として機能するICチップであるCPU300と、操作パネルである入力部301と、データ送信伝送回路である送信部303と、LEDにより表示をおこなう表示部302と、記憶部310とを備える。

【0158】

CPU300は、データの入出力、データ送信、換算定数選択処理、データの暗号化、信号生成処理等の制御を行う。入力部301は、テンキーと、例えば「OPN」（開）スイッチ、「CLS」（閉）スイッチ、登録スイッチ、送信スイッチのように、ある機能に特化されたスイッチや、その他の入力スイッチを有する。

【0159】

表示部302は、CPU300の出力に従いLEDによる表示を行う。送信部

303は、装置4へデータ信号の送信を行う信号発信素子を有する。記憶部310は、個人認証番号A、CPU300の制御プログラム、パターン換算定数データ310a等のデータが格納されており、また作業領域として機能するように構成されている。

【0160】

なお、個人認証番号Aは送信者が有する認証カードに記憶され、装置3が個人認証番号Aを認証カードから接触又は非接触等の方式によって読取るように構成してもよい。

【0161】

装置4は、制御部であるCPU400と、操作パネル及び設定パネルを有する入力部401と、LCD表示器である表示部402と、装置3からのデータ信号を受信する受信部403と、記憶部410と、外部駆動装置とのインターフェース部404とを備える。

【0162】

CPU400は、データの入出力制御、データ受信制御、データ読取処理、データの復号化、認証処理、外部駆動装置への駆動信号送出の制御等を行う。入力部401は、各種入力スイッチから構成され、テンキー、アルファベットキー、特定の機能に特化したスイッチ（例えば、電源ON/OFFスイッチ、ドア開閉スイッチ等）等を有する。

【0163】

表示部402は、CPU400からの出力に従い復号化データや、操作時の入力データ等の表示を行う。受信部403は、装置3からのデータ受信を行う受信ヘッドを有する。

【0164】

記憶部410は、個人認証番号A、パターン換算定数データ410a、CPU400の制御プログラム等が記憶されており、またプログラムの作業領域として機能するように構成されている。パターン換算定数データ410aは装置3が有するパターン換算定数データ310aと同様のものである。なお、装置3からパターン換算定数データを装置4に送信して登録することができるようになってい

る。

【0165】

装置3と装置4の間のデータ送信方式は、赤外線方式に限らず、無線電波方式、光通信方式、有線通信方式等が適用可能である。

【0166】

外部駆動装置である電子錠5は、装置4のインターフェース部404と接続されており、装置4からの解錠駆動信号により電子ロックの解錠操作を行い、施錠駆動信号により電子ロックの施錠操作を行う。また、外部駆動装置として電子錠5を複数接続することも可能である。

【0167】

次に、図21及び図22に基づき、装置3から装置4へ送信される第1信号 S_1 及び第2信号 S_2 について説明する。上述の実施例と重複する部分については説明を省略する。第1信号 S_1 及び第2信号 S_2 は、パケット0乃至4の5つのデータ領域を有する。パケット0は、通信番号格納領域である。パケット1は、換算定数 X 又は Y の格納領域である。パケット2は、パターン換算定数 Z_y の格納領域である。パターン換算定数 Z_y は、第2信号 S_2 のみに格納される。

【0168】

パケット3は、個人ID代替値 A_x 又は A_y が格納される領域である。パケット4は、解錠又は施錠を表すON/OFF信号格納領域である。信号としては、解錠を表す「1」、施錠を表す「0」がある。なお、複数の電子錠5を操作する場合は、各々の電子錠5を区別するためのパケット領域を設けるとよい。

【0169】

該パケットに、各々の電子錠5に対して与えられた登録番号を格納し、該登録番号によって装置4から駆動信号を出力する電子錠5を区別するように構成することができる。

【0170】

換算定数 X 、 Y 、 Z_y を用いて個人認証番号 A を暗号化する方法については、上述の実施例と同様である。なお、本例では、ON/OFF信号を暗号化することはしていないが、個人認証番号 A と同様に暗号化してもよい。また、パター

ン換算定数 Z_y 及び対応する換算定数 $Z_{y'}$ の組合せデータは、装置 3 及び装置 4 にそれぞれ登録されている。

【0171】

次に本システム S-2 の動作について説明する。送信者が、装置 3 の入力部 301 から解錠又は施錠データを入力 (OPN (開) スイッチ又はCLS (閉) スイッチを押下) すると、表示部 302 にその旨が表示 (「OPEN」又は「CLOSE」表示) される。次に、送信者はパターン換算定数 Z_y を指定するためのスイッチ操作をして (例えば、 $Z_y = \text{「g」}$)、入力部 301 の送信スイッチを押下する。

【0172】

CPU300 は、送信スイッチが押下されたタイミングで乱数により換算定数 X, Y を選択し (例えば、 $X = 1122$, $Y = 3344$)、また、指定されたパターン換算定数 Z_y に対応する換算定数 $Z_{y'}$ (例えば、 $Z_{y'} = 3399$) を選択する。なお、換算定数 $Z_{y'}$ は CPU300 によって自動選択されるようにしてもよい。

【0173】

次に、CPU300 は、換算定数 X, Y, $Z_{y'}$ によって個人認証番号 A を暗号化する。図 20 及び図 21 に示された例では、個人 ID 代替値 A_x は「12352421」 ($A_x = A + Y + Z_{y'}$)、個人 ID 代替値 A_y は「12350199」 ($A_y = A + X + Z_{y'}$) となる。そして、この暗号化データ等が組合せ配置され、第 1 信号 S_1 及び第 2 信号 S_2 が生成される。なお、個人認証番号 A を暗号化するための第 1 式を $A_x = A + Y + Z_{y'}$ とし、第 2 式を $A_y = A + X$ としてもよく、又、第 1 式を $A_x = A + Y$ とし、第 2 式を $A_y = A + X + Z_{y'}$ としてもよい。

【0174】

第 1 信号 S_1 及び第 2 信号 S_2 が生成されると、CPU300 は、該信号を送信部 303 から装置 4 の受信部 403 へ向けて、所定時間ずらしてそれぞれ送信する。このとき、それぞれの信号を複数回づつ送信してもよい。また、装置 3 及び装置 4 に送受信部を設け、装置 3 から装置 4 へ第 1 信号 S_1 が送信されると、

装置4から装置3へアンサーバック信号が返信され、所定時間以内の該アンサーバック信号の受信を条件に装置3から装置4へ第2信号 S_2 が送信されるように構成してもよい。

【0175】

装置4では、受信部403により第1信号 S_1 及び第2信号 S_2 が所定時間内に受信されると、該信号はCPU400によって読取られる。CPU400は、それぞれの信号の通信番号（パケット0）が一致するか否かを判別し、一致した場合は認証及び復号化処理へ移行する。しかし、通信番号は一致しなかった場合は、処理を終了する。このとき、通信番号が一致しなかった旨を音声により報知するようにしてもよい。なお、装置4への両信号の送信に先立ち、送信者のパスワードを装置4へ入力し、該パスワードが正しく認証されたことを条件として、装置4が両信号を受信可能とするように構成してもよい。

【0176】

通信番号が一致すると、パターン換算定数データ410aを参照して、CPU400によって第2信号 S_2 のパターン換算定数 Z_y に対応する換算定数 $Z_{y'}$ が読み込まれる。そして、個人ID代替値 A_x 、 A_y がそれぞれ換算定数 Y と $Z_{y'}$ 、換算定数 X と $Z_{y'}$ によって復号化される。そして、それぞれから得られた復号化データ A_1 （ $A_1 = A_x - Y - Z_{y'}$ ）と A_2 （ $A_2 = A_y - X - Z_{y'}$ ）が一致するか否かが判別される。また、別の暗号化式では、復号化データ $A_1 = A_x - Y - Z_{y'}$ 、 $A_2 = A_y - X$ 、又は、復号化データ $A_1 = A_x - Y$ 、 $A_2 = A_y - X - Z_{y'}$ となる。

【0177】

両復号化データが一致した場合は、送信者が正規の送信者であると認証され、CPU400はON/OFF信号（パケット4）に基づいてインターフェース部404を介して、外部駆動装置（電子錠5）へ解錠／施錠駆動信号を送出する。一方、両復号化データが一致しなかった場合は、成りすまし者からの不正信号であると判別され、音声による報知がなされるように構成されている。

【0178】

なお、両復号化データが一致しさらに、装置4が記憶している個人認証番号A

と復号化データが一致した場合に、送信者が正規の送信者であると認証されるようにしてもよい。このようにすることにより、さらに有効的に成りすまし送信を排除することができる。

【0179】

以上のように、装置3と装置4に共通のパターン換算定数データ310a及び410aが記憶されており、第1信号 S_1 及び第2信号 S_2 に含まれて送信される換算定数 X 、 Y 以外に、換算定数 $Z_{y'}$ が暗号化に用いられている。したがって、仮に成りすまし送信信号が同様のデータ配置からなるものであったとしても、換算定数 X 、 Y 及び $Z_{y'}$ による暗号化式、パターン換算定数 Z_y と換算定数 $Z_{y'}$ との対応関係がわからない限り、装置4では不正な信号を受信したと判断される。

【0180】

このように、本システムS-2では、成りすまし送信によっては装置4及び電子錠5は操作できないようになっているので、高い安全性を確保することが可能となる。

【0181】

【発明の効果】

以上のように本発明によれば、第1のデータ送信方法として、送信側装置から送信データの送信が行われるとき、暗号化された送信データをそれぞれ含む第1信号と第2信号が設定され、それらは別々のルートで送信される。第1信号には、第2の換算定数と第3の換算定数（又は第2の換算定数のみ）によって暗号化された送信データの代替値と、第1の換算定数と、が配置され送信される。一方、第2信号には、第1の換算定数と第3の換算定数（又は第1の換算定数のみ）によって暗号化された送信データの代替値と、第2の換算定数と、第3の換算定数と対応関係にあるパターン換算定数と、が配置され送信される。

【0182】

したがって、それぞれの信号が別ルートで送信されるので、安全性が確保されるのに加え、第1信号及び第2信号には、第3の換算定数自体は含まれておらず、仮に双方の信号が漏洩した場合であっても、第3者による送信データの復号化

を行うことはできず、秘匿性が確保される。

【0183】

そして、第2信号は中継装置へ一旦送信され、第2信号に含まれるパターン換算定数が対応する第3の換算定数に変換され、この信号は受信側装置へ転送される。したがって、送信側では、送信側装置にパターン換算定数と第3の換算定数との対応データを登録しておくと共に、中継装置にも同様のデータを登録しておけば、中継装置で第2信号を変換することができる。

【0184】

このようにすることにより、送信データの秘匿性を確保できると共に、さらに複数のパターン換算定数を登録しておくことによりさらに秘匿性を高めることができる。また、受信側装置には、受信側装置のパターン換算定数を登録しておく必要がないので、送信側装置から複数の受信側装置に対して同一のパターン換算定数を使用して暗号化することも可能であり、暗号化に対する自由度が高まる。

【0185】

また、認証データの暗号化、復号化は、換算定数による容易なものであるにも関わらず、安全なデータ送信が可能であり、データ送信に係る構成が簡単であるため、コストが掛からずにデータ送信システムを構築することができる。

【0186】

また、本来の送信者になりかわって第3者がデータを送信したとしても、パターン換算定数及び第3の換算定数との対応関係がわからない限り、受信側装置では、両信号から送信データを復号したときに、有意なデータとして復号化できないので、容易に成りすまし送信であることが判別できる。

【0187】

また、受信側装置では、送信側装置からの第1信号と中継装置からの第2'信号を組み合わせることにより復号化が可能であるので、中継装置を介さずに第2'信号が送信されてきた場合にも、送信者アドレスからも成りすまし送信であることを判別可能である。

【0188】

また、第2のデータ送信方法として、中継装置を介さずに送信側装置から受信

側装置へ第1信号及び第2信号が送信される場合にも、第1の換算定数、第2の換算定数及び第3の換算定数が用いられて送信データが暗号化され、第1及び第2の換算定数は第1信号又は第2信号に含められて送信されるが、第3の換算定数自体は送信されず、その代わりに第3の換算定数に対応するパターン換算定数が送信信号に含められる。

【0189】

そして、送信側装置及び受信側装置の双方にパターン換算定数を登録しておくことにより、受信側装置では、受信信号に含められたパターン換算定数に対応する第3の換算定数を知ることができ、第1信号及び第2信号から送信データを復号化することができる。

【0190】

このようにすることにより、送信途中で第1信号及び第2信号が漏洩した場合であってもパターン換算定数に対応する第3の換算定数を知らない第三者は、送信データを復号化することができず秘匿性を確保することができる。

【0191】

また、成りすまし送信された場合には、成りすまし送信の第2信号に含められたパターン換算定数と送信データを暗号化した第3の換算定数との関係が、正規のパターン換算定数と第3の換算定数の関係に一致しないので、両信号から復号化された復号化データが有意なデータとして復号化できないので、容易に成りすまし送信であることを判別可能である。

【0192】

以上のように、本発明によれば、本来の送信者になりかわって第三者がデータを送信しても、受信者側で送信者の個人認証を行うことにより送信者を特定し、上記成りすまし送信による不都合を防ぐことができると共に、秘匿性の高いデータ送信システム及びデータ送信方法並びに装置を提供することができる。

【図面の簡単な説明】

【図1】

第1のデータ送信方法の説明図である。

【図2】

第2のデータ送信方法の説明図である。

【図3】

実施例のデータ送信システムの説明図である。

【図4】

実施例のデータ送受信側装置の構成図である。

【図5】

実施例の送信データの暗号化についての説明図である。

【図6】

実施例の第1信号の構成を表す説明図である。

【図7】

実施例の第2信号の構成を表す説明図である。

【図8】

実施例の送信側装置のパターン換算定数データの説明図である。

【図9】

実施例の中継装置パターン換算定数データの説明図である。

【図10】

実施例の第2'信号の構成を表す説明図である。

【図11】

実施例の送信信号の復号化についての説明図である。

【図12】

実施例の送信信号の復号化についてのデータ例を示す説明図である。

【図13】

実施例の送信側装置の処理の流れを示す説明図である。

【図14】

実施例の中継装置の処理の流れを示す説明図である。

【図15】

実施例の受信側装置の処理の流れを示す説明図である。

【図16】

実施例の受信側装置の処理の流れを示す説明図である。

【図 17】

第 1 のデータ送信方法の変形例を表す説明図である。

【図 18】

第 1 のデータ送信方法の変形例を表す説明図である。

【図 19】

別実施例のデータ送信システムの説明図である。

【図 20】

別実施例のデータ送信システムの構成装置の構成図である。

【図 21】

別実施例の第 1 信号の構成を表す説明図である。

【図 22】

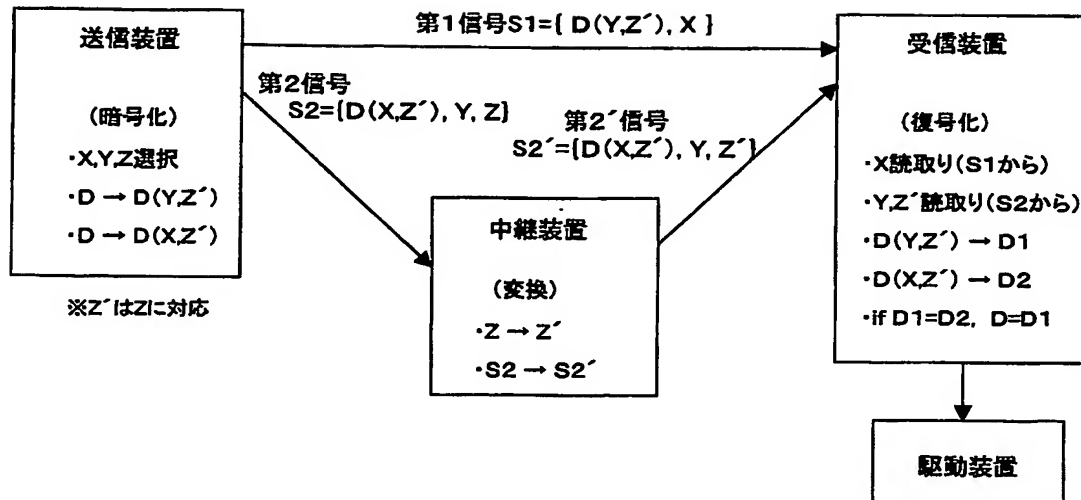
別実施例の第 2 信号の構成を表す説明図である。

【符号の説明】

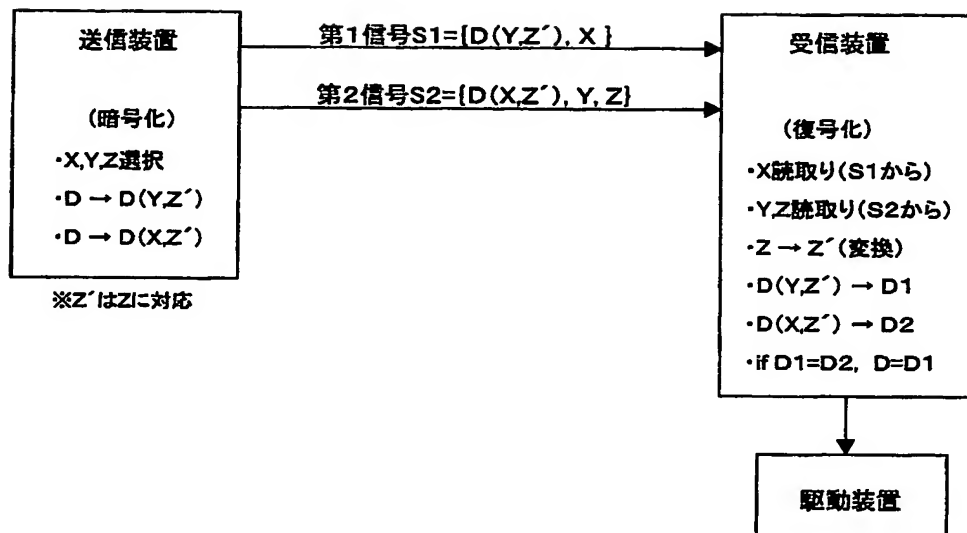
1, 3, 4 装置、2 中継装置、5 電子錠、100, 200, 300, 400 CPU、101, 201 入出力部、102, 202, 302, 402 表示部、103, 203 送受信部、110, 210, 310, 410 記憶部、111a, 211a, 310a, 410a パターン換算定数データ、111, 211 主記憶部、301, 401 入力部、303 送信部、403 受信部、404 インターフェース部、A 個人認証番号、B 搬送認証番号、C 制御データ、Dt 機密データ、Ax, Ay 個人ID代替値、Bx, By 搬送ID代替値、Cx, Cy 制御データ代替値、Cp 制御パターン、A1, B1, C1, D1, A2, B2, C2, D2 復号化データ、I インターネット、P プロバイダ、S, S-2 システム、S1 第1信号、S2 第2信号、X, Y, Zx, Zy 換算定数、Zx', Zy' パターン換算定数

【書類名】 図面

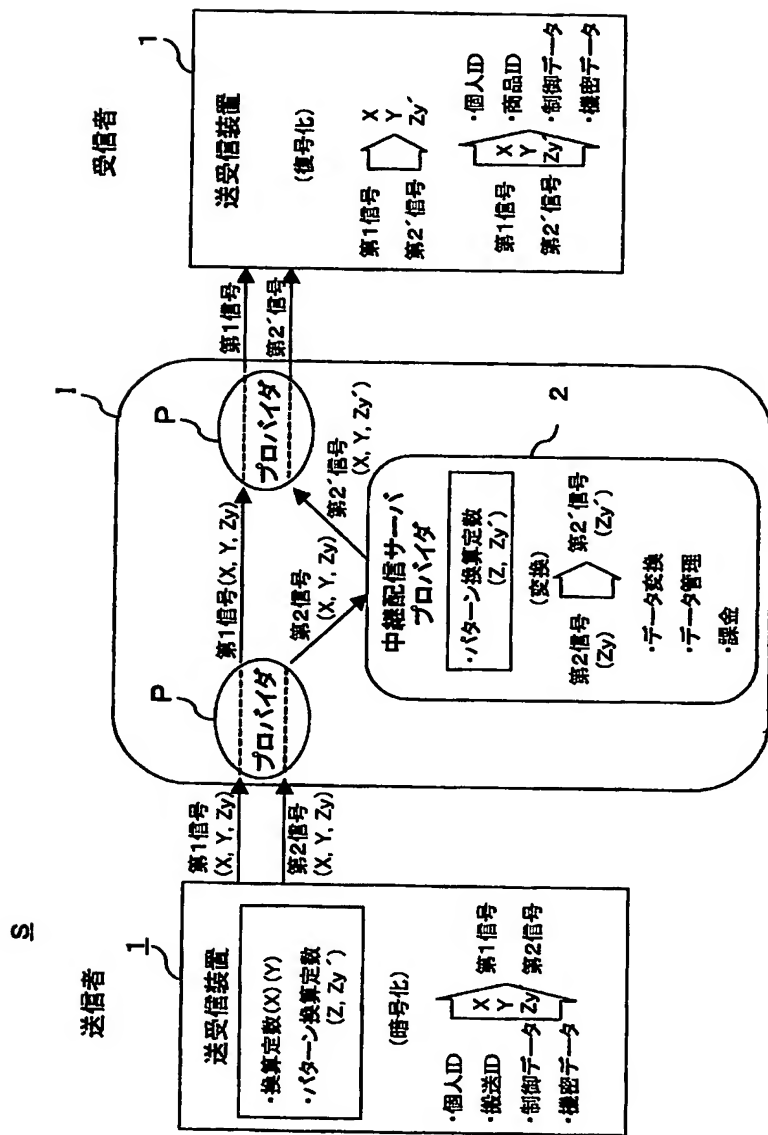
【図 1】



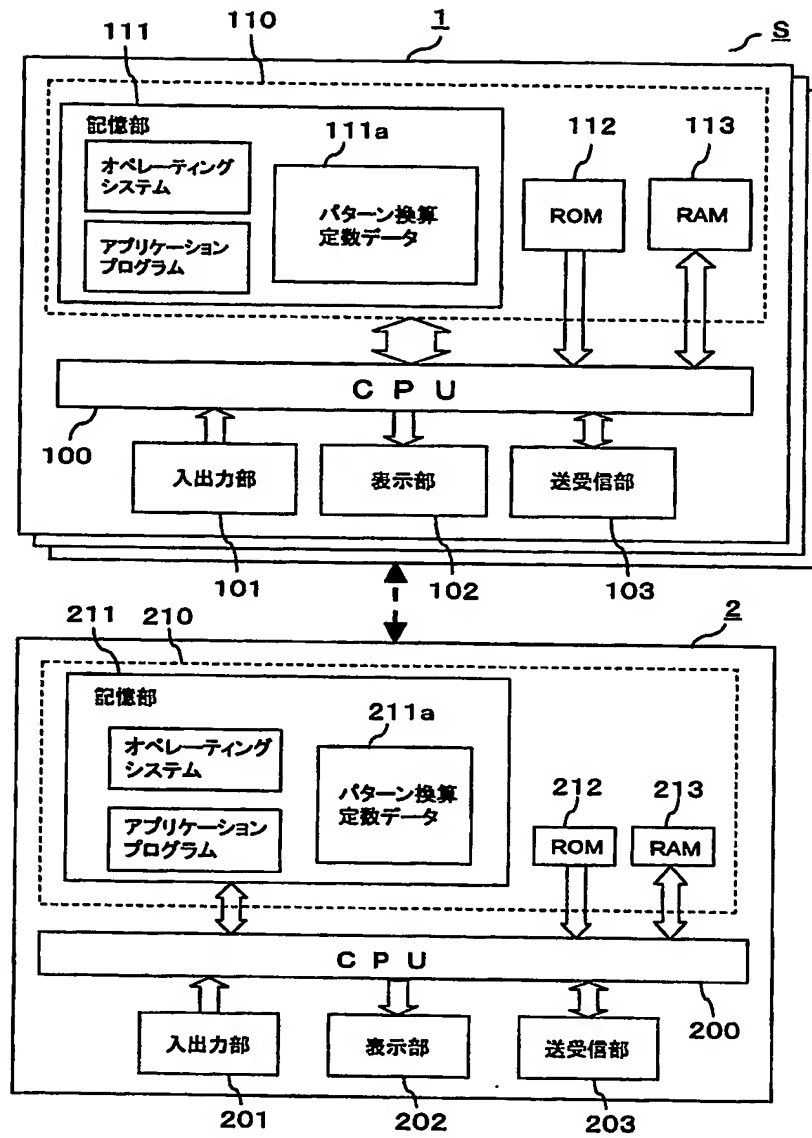
【図 2】



【図 3】



【図 4】

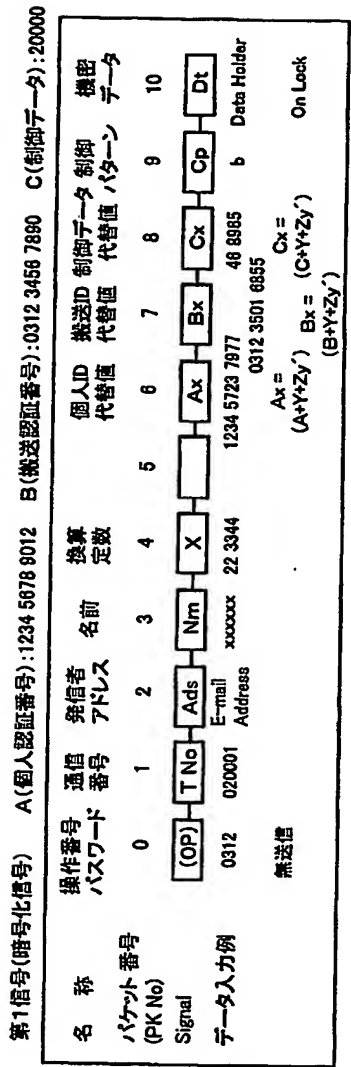


【図 5】

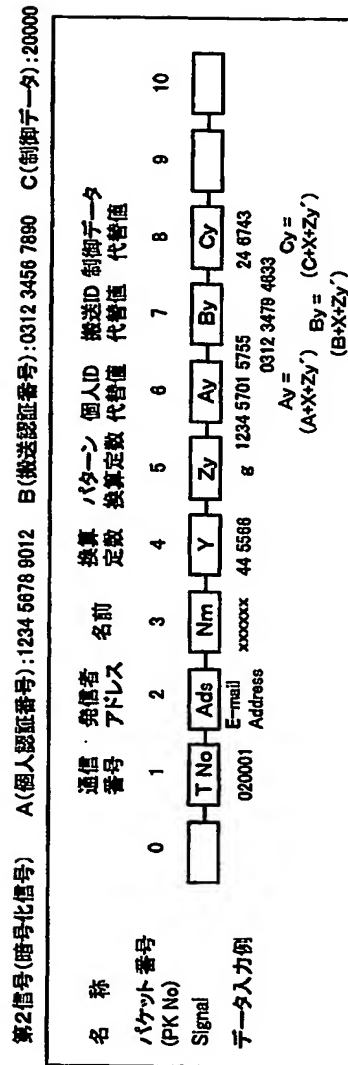
信号暗号化 A(個人認証番号):1234 5678 9012 B(搬送認証番号):0312 3456 7890 C(制御データ):20000		
暗号化データ	復号式	信号暗号化データ例
A個人IDデータ	第1式 $A_x = A + Y + Z_y'$	1234 5723 7977 = (1234 5678 9012) + (44 5566) + (3399)
	第2式 $A_y = A + X + Z_y'$	1234 5701 5755 = (1234 5678 9012) + (22 3344) + (3399)
B搬送IDデータ	第1式 $B_x = B + Y + Z_y'$	0312 3501 6855 = (0312 3456 7890) + (44 5566) + (3399)
	第2式 $B_y = B + X + Z_y'$	0312 3479 4633 = (0312 3456 7890) + (22 3344) + (3399)
C制御データ	第1式 $C_x = C + Y + Z_y'$	46 8965 = (2 0000) + (44 5566) + (3399)
	第2式 $C_y = C + X + Z_y'$	24 6743 = (2 0000) + (22 3344) + (3399)

X, Y, Z_{y'}:換算定数

【図 6】



【図 7】

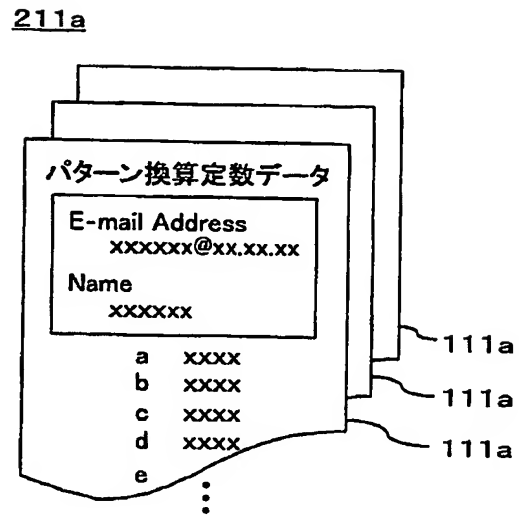


【図 8】

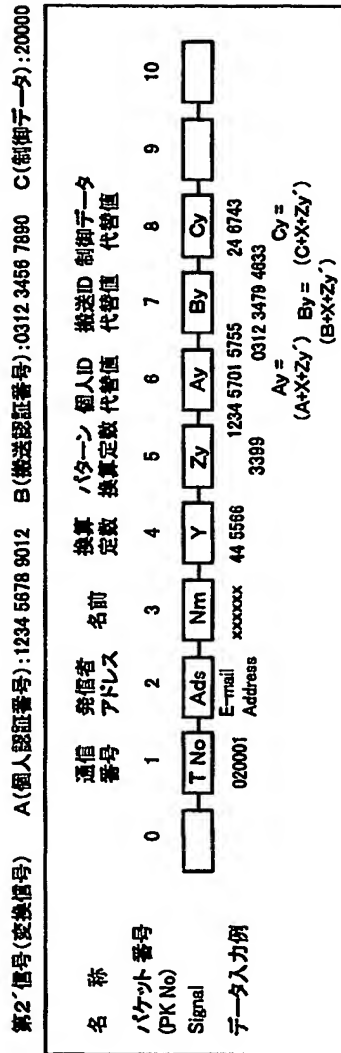
111a

パターン換算定数データ	
a	1234
b	2345
c	3456
⋮	
g	3399
h	4400
⋮	
z	9911

【図 9】



【図 10】



【図 1 1】

信号復号化

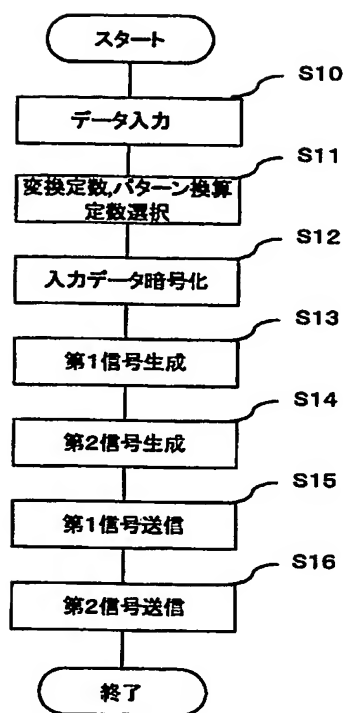
復号化データ	復号式	認証
A個人IDデータ	第1式 $Nm / Ax - Y - Zy' = A1$	$A1 = A2$
	第2式 $Nm / Ay - X - Zy' = A2$	
B搬送IDデータ	第1式 $Bx - Y - Zy' = B1$	$B1 = B2$
	第2式 $By - X - Zy' = B2$	
C制御データ	第1式 $Cx - Y - Zy' = C1$	$C1 = C2$
	第2式 $Cy - X - Zy' = C2$	

【図 1 2】

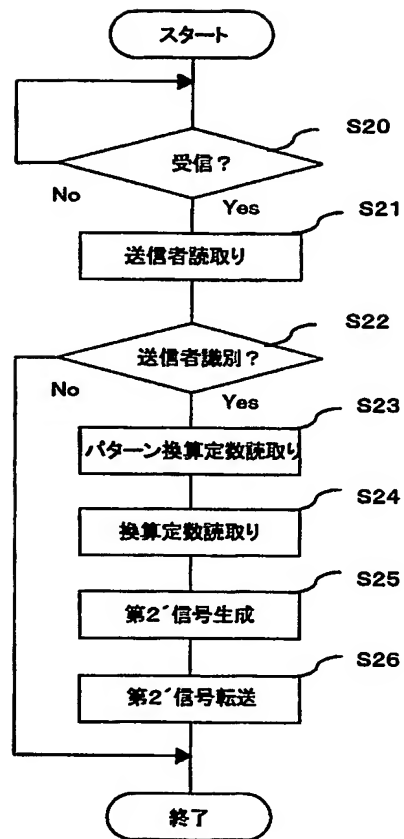
信号復号化データ例 A(個人認証番号):1234 5678 9012 B(搬送認証番号):0312 3456 7890 C(制御データ):20000

A個人IDデータ	第1式 $Nm \quad Ax \quad Y \quad Zy' \quad A1$ (xxxxxx)/(1234 5723 7977)-(44 5566)-(3399) = xxxxxx/1234 5678 9012
	第2式 $Nm \quad Ay \quad X \quad Zy' \quad A2$ (xxxxxx)/(1234 5701 5755)-(22 3344)-(3399) = xxxxxx/1234 5678 9012
B搬送IDデータ	第1式 $Bx \quad Y \quad Zy' \quad B1$ (0312 3501 6855)-(44 5566)-(3399) = 0312 3456 7890
	第2式 $By \quad X \quad Zy' \quad B2$ (0312 3479 4633)-(22 3344)-(3399) = 0312 3456 7890
C制御データ	第1式 $Cx \quad Y \quad Zy' \quad C1$ (46 8965)-(44 5566)-(3399) = 2 0000 (¥20,000)
	第2式 $Cy \quad X \quad Zy' \quad C2$ (24 6743)-(22 3344)-(3399) = 2 0000 (¥20,000)

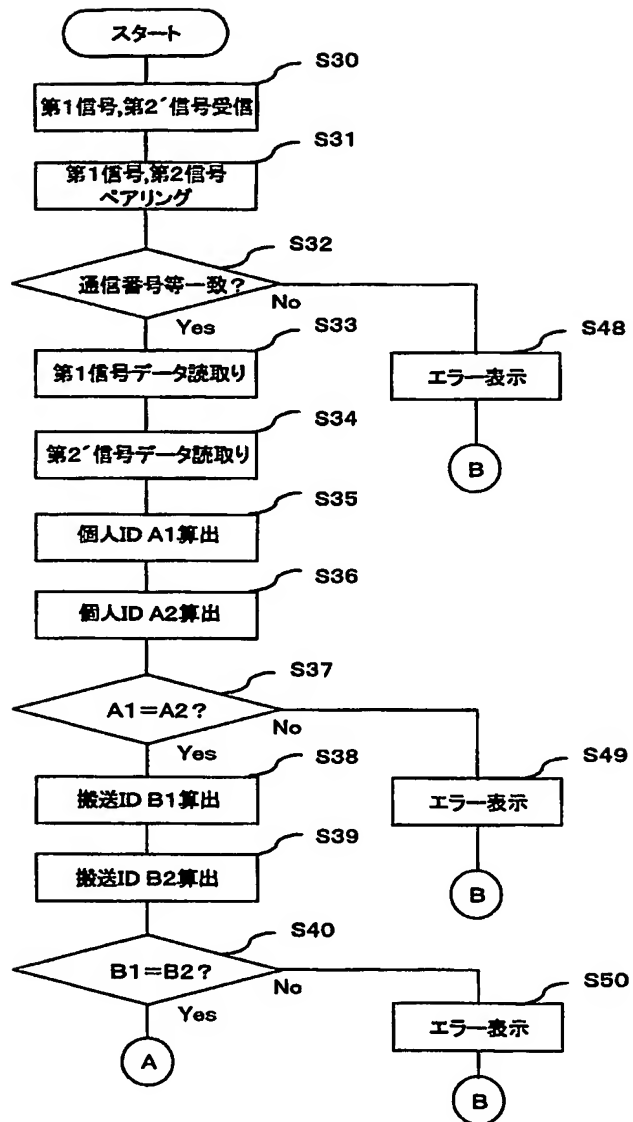
【図 13】



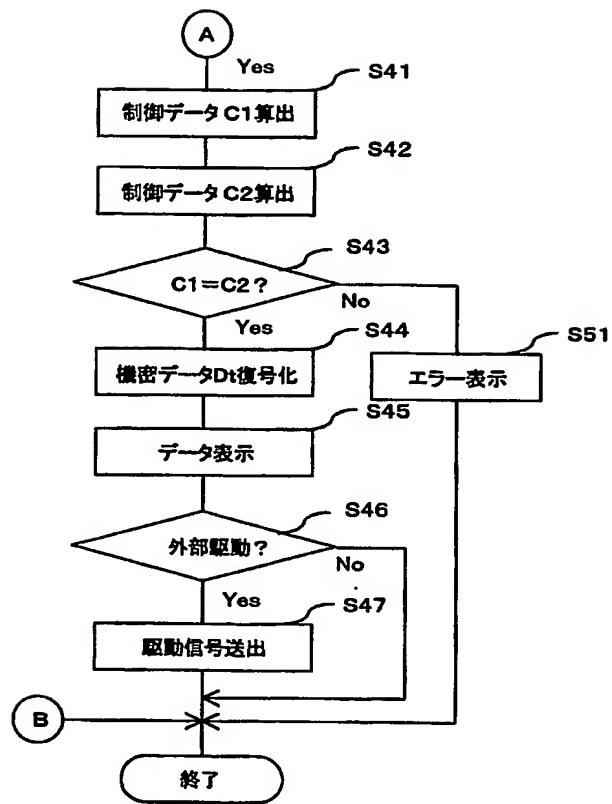
【図 14】



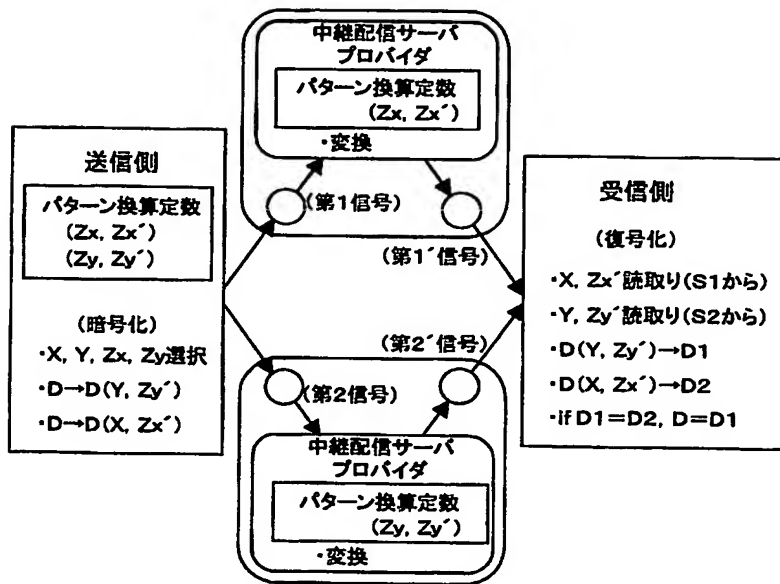
【図 15】



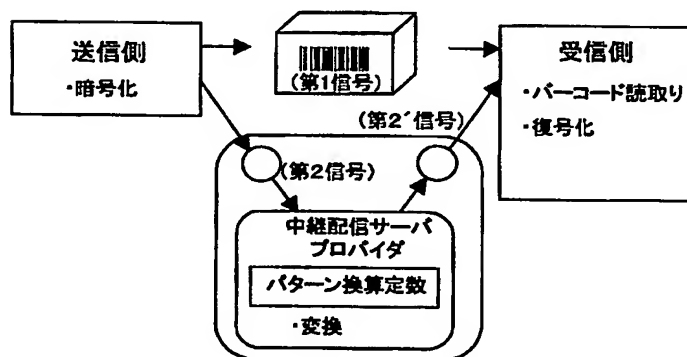
【図 16】



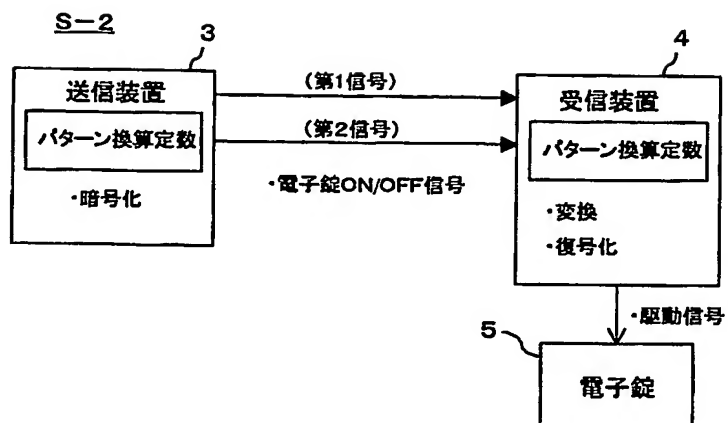
【図 17】



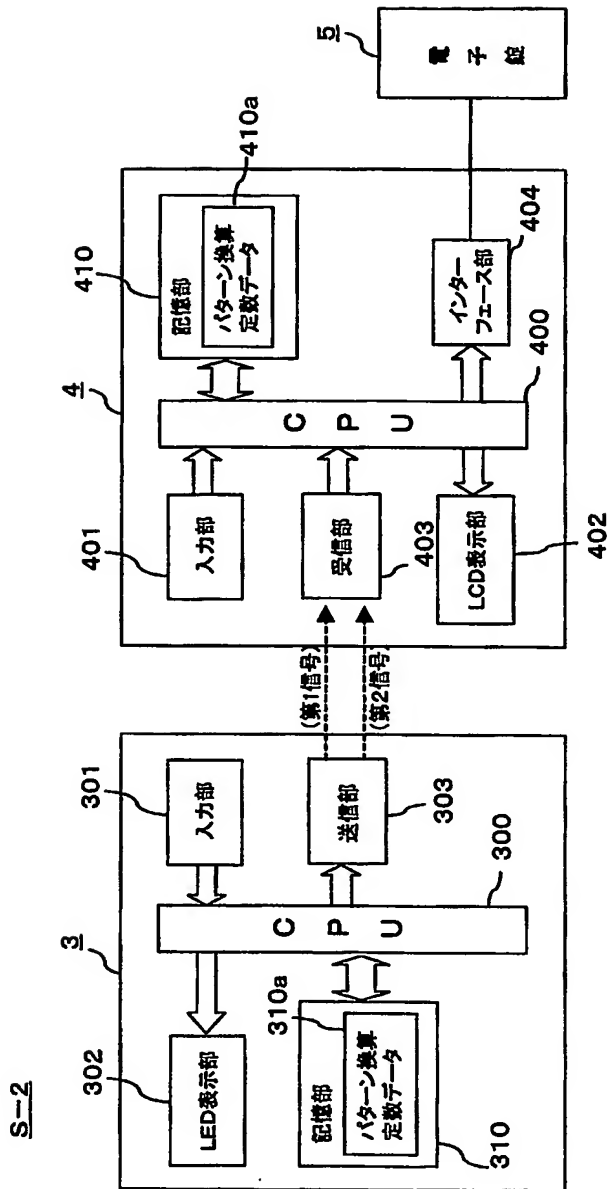
【図 18】



【図 19】.



【図 20】



【図 2 1】

第1信号(暗号化信号) A(個人認証番号):1234 5678 B(ON/OFF信号):1又は0

名 称	通信 番号	換算 定数	個人ID 代替値	ON/OFF 信号	
パケット 番号 (PK No)	0	1	2	3	4
Signal	<div>TNoX<div></div>AxB</div>				
データ入力例	001	1122	1235 2421	1	
<div>Ax = (A+Y+Zy') ON信号</div>					

【図 2 2】

第2信号(暗号化信号) A(個人認証番号):1234 5678 B(ON/OFF信号):1又は0

名 称	通信 番号	換算 定数	パターン 換算定数	個人ID 代替値	
パケット 番号 (PK No)	0	1	2	3	4
Signal	<div>TNoYZyAy</div>				
データ入力例	001	3344	g	1235 0199	
<div><div>g-3399</div><div>Ay = (A+X+Zy')</div></div>					

【書類名】 要約書

【要約】

【課題】 送信データの秘匿性を高めると共に、成りすまし送信を効果的に排除することができるデータ送信システム及びデータ送信方法並びに装置を提供する。

【解決手段】 送信側装置 1 から受信側装置 1 へ換算定数 Y , $Z_{y'}$ による暗号化データと、換算定数 X と、を含む第 1 信号 S_1 が送信され、送信側装置 1 から中継装置 2 へ換算定数 X , $Z_{y'}$ による暗号化データと、換算定数 Y と、換算定数 $Z_{y'}$ のパターン換算定数 Z_y と、を含む第 2 信号 S_2 が送信され、第 2 信号 S_2 のパターン換算定数 Z_y が換算定数 $Z_{y'}$ へ変換された第 2' 信号 $S_{2'}$ が中継装置 2 から受信側装置 1 へ転送され、受信側装置 1 では、第 1 信号 S_1 及び第 2' 信号 $S_{2'}$ により暗号化データ及び換算定数 X , Y , $Z_{y'}$ が読取られ、暗号化データの復号化及び認証が行われる。

【選択図】 図 3

認定・付加情報

特許出願の番号	特願 2003-010183
受付番号	50300073474
書類名	特許願
担当官	第八担当上席 0097
作成日	平成15年 1月20日

<認定情報・付加情報>

【提出日】	平成15年 1月17日
-------	-------------

次頁無

特願2003-010183

出願人履歴情報

識別番号

[500400700]

1. 変更年月日

2000年 7月25日

[変更理由]

新規登録

住所

東京都葛飾区東金町1-36-1-1318

氏名

加藤 誠